EXHIBIT 2

8-K 1 d734596d8k.htm FORM 8-K

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): July 19, 2019

Equifax Inc.
(Exact Name of Registrant as Specified in Charter)

Georgia	001-06605	54-0401110
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(IRS Employer Identification No.)

1550 Peachtree Street, N.W. Atlanta, Georgia	30309
(Address of Principal Executive Offices)	(Zip Code)

Registrant's telephone number, including area code: (404) 885-8000

Not Applicable
(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol	Name of each exchange on which registered
Common stock, $1.25 par value per share	**EFX**	**New York Stock Exchange**

Indicate by check mark whether the registrant is an emerging growth company as defined in as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 1.01. Entry into a Material Definitive Agreement.

As previously disclosed, Equifax Inc. (the "Company") has been a party to a significant number of legal proceedings and investigations in connection with a cybersecurity incident in 2017 following a criminal attack on the Company's systems that involved the theft of certain personally identifiable information of consumers.

On July 19, 2019 and July 22, 2019, the Company entered into multiple agreements that resolve a class action lawsuit filed on behalf of U.S. consumers captioned *In re: Equifax, Inc. Customer Data Security Breach Litigation, MDL No. 2800 (Consumer Cases)* (the "U.S. Consumer Litigation") and the investigations of the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), the Attorneys General of 48 states, the District of Columbia and Puerto Rico (the "MSAG Group") and the New York Department of Financial Services ("NYDFS") (collectively, the "Consumer Settlement").

Under the terms of the Consumer Settlement, the Company will contribute $380.5 million to a non-reversionary settlement fund (the "Consumer Restitution Fund") to provide restitution for U.S. consumers identified by the Company whose personal information was compromised as a result of the 2017 cybersecurity incident (the "affected consumers").

The Consumer Restitution Fund will be used to (1) compensate affected consumers for certain unreimbursed costs or expenditures incurred by affected consumers that are fairly traceable to the 2017 cybersecurity incident, (2) provide affected consumers with an opportunity to enroll in at least four years of credit monitoring services provided by a third party unaffiliated with the Company or alternative compensation for affected consumers who already have other credit monitoring services, (3) provide affected consumers with additional benefits such as identity restoration services and (4) pay reasonable attorneys' fees and reasonable costs and expenses for the plaintiffs' counsel in the U.S. Consumer Litigation (not to exceed $80.5 million) and administrative and notice costs.

The Company has agreed to contribute up to an additional $125 million to the Consumer Restitution Fund to cover unreimbursed costs and expenditures described in (1) above in the event the $380.5 million in the Consumer Restitution Fund is exhausted. In addition, if the number of affected consumers who enroll in the third party credit monitoring services described above in (2) exceeds seven million, the Company may be required, under certain circumstances, to contribute additional money into the Consumer Restitution Fund to cover the incremental cost of providing credit monitoring services to the additional affected consumers.

The Company also agreed to pay an additional $180.5 million to the MSAG Group and the following monetary penalties: (1) $100 million to the CFPB and (2) $10 million to the NYDFS.

The Company also agreed to implement certain business practice commitments related to information security to safeguard the personal information of consumers, including conducting third party assessments of its information security program.

The Consumer Settlement, other than the agreement with the NYDFS, is subject to court approval. The agreements regarding the U.S. Consumer Litigation and the FTC and CFPB investigations are subject to approval by the U.S. District Court for the Northern District of Georgia (the "Court"). The settlement with the MSAG Group consists of substantially similar agreements with each of the participating jurisdictions, and each agreement is subject to court approval in the relevant jurisdiction. There can be no assurance that the courts in each relevant jurisdiction will approve the agreements which make up the Consumer Settlement.

The Company expects to pay the MSAG Group, the CFPB and the NYDFS in the third quarter of 2019. The Company will establish and contribute approximately $25 million to the Consumer Restitution Fund promptly after the Court approves the issuance of notice of class action settlement. That preliminary Court approval is expected in the third quarter of 2019. The contribution of the remainder of the $380.5 million to the Consumer Restitution Fund will be made after final Court approval of the Consumer Settlement, which could occur as early as the fourth quarter of 2019. The timing of the final Court approval of the settlement agreement for the U.S. Consumer Litigation cannot be predicted with certainty as it will depend on a number of factors outside of our control, including the number of objections, if any, to the settlement agreement, the Court's schedule and discretion, and any appeals, among other factors. Our current plans are to finance the payments with existing borrowing capacity, including under our $1.1 billion five-year unsecured revolving credit facility and our $225 million receivables funding facility.

The Company's participation in the Consumer Settlement does not constitute an admission by the Company of any fault or liability, and the Company does not admit fault or liability.

If approved by an applicable court, the Consumer Settlement will only resolve the U.S. Consumer Litigation and the investigations of the FTC, CFPB, MSAG Group and NYDFS. All other legal proceedings and investigations found under the caption "Legal Proceedings" in the Company's Quarterly Report on Form 10-Q for the quarter ended March 31, 2019 as filed with the Securities and Exchange Commission on May 10, 2019, other than as specifically stated therein, remain ongoing.

Item 2.02. Results of Operations and Financial Condition.

As previously disclosed, the Company recorded an accrual of $690 million in selling, general, and administrative expenses and other current liabilities in our Consolidated Statements of (Loss) Income and Balance Sheets as of and for the period ended March 31, 2019, respectively, exclusive of its legal and professional services expenses, for losses associated with certain legal proceedings and government investigations related to the 2017 cybersecurity incident. Principally as a result of the Consumer Settlement described above, the Company expects to increase its accrual with respect to these matters by approximately $11 million in the second quarter of 2019.

Forward-Looking Statements

This Current Report on Form 8-K contains forward-looking statements and forward-looking information. These statements can be identified by expressions of belief, expectation or intention, as well as statements that are not historical fact. These statements are based on certain factors and assumptions. While the company believes these factors and assumptions to be reasonable based on information currently available, they may prove to be incorrect.

Several factors could cause actual results to differ materially from those expressed or implied in the forward-looking statements, including, but not limited to, potential adverse developments in new and pending legal proceedings or government investigations, including the failure to obtain final court approval of the agreements which make up the Consumer Settlement; uncertainties regarding the ultimate amount and timing of payments the Company may be required to make in connection with the Consumer Settlement; the cost of compliance with the Company's non-monetary obligations associated with the Consumer Settlement; uncertainties regarding the outcome of the remaining legal proceedings or government investigations related to the 2017 cybersecurity incident; and limitations on the Company's ability to access the capital markets and corresponding effects on the Company's ability to finance its obligations. A summary of additional risks and uncertainties can be found in the Company's Annual Report on Form 10-K for the year ended December 31, 2018, including without limitation under the captions "Item 1. Business — Governmental Regulation" and "— Forward-Looking Statements" and "Item 1A. Risk Factors," and in the Company's other filings with the U.S. Securities and Exchange Commission. Forward-looking statements are given only as at the date of this release and the company disclaims any obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise, except as required by law.

Item 9.01. Financial Statements and Exhibits.

(d) Exhibits

10.1*	Settlement Agreement and Release dated July 22, 2019 between the Company and the Settlement Class Representatives (as defined therein).
10.2*	Stipulated Order for Permanent Injunction and Monetary Judgment dated July 19, 2019 between the Company and the Federal Trade Commission.
10.3*	Stipulated Order for Permanent Injunction and Monetary Judgment dated July 19, 2019 between the Company and the Bureau of Consumer Financial Protection.
10.4	Final Judgment and Consent Decree dated July 19, 2019 between the Company and the State of Alabama, with a schedule of the additional jurisdictions in which such agreement (consent decrees) have been approved that are substantially identical in all material respects.

* Schedules and exhibits to this agreement have been omitted pursuant to Item 601(a)(5) of Regulation S-K. A copy of any omitted schedule and/or exhibit will be furnished as a supplement to the Securities and Exchange Commission upon request.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Equifax Inc.

By: /s/ John J. Kelley III
Name: John J. Kelley III
Title: Corporate Vice President, Chief Legal Officer and Corporate Secretary

Date: July 22, 2019

EX-10.2 3 d734596dex102.htm EX-10.2

Exhibit 10.2

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

EQUIFAX INC.,

Defendant.

Case No. _____

STIPULATED ORDER FOR PERMANENT INJUNCTION AND MONETARY JUDGMENT

Plaintiff, the Federal Trade Commission ("Commission"), filed its Complaint for a permanent injunction and other relief in this matter, pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b). The Commission and Defendant Equifax Inc. ("Defendant") stipulate to entry of this Order for Permanent Injunction and Monetary Judgment ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendant engaged in acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Sections 501(b) and 505(b)(2) of the Gramm-Leach-Bliley Act ("GLB Act"), and 15 U.S.C. §§ 6801(b) and 6805(6b)(2), by failing to reasonably secure sensitive consumer personal information in Defendant's networks and computer systems.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorneys' fees.

5. Defendant and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

1. "**Affected Consumer**" means the approximately One Hundred Forty Seven Million (147,000,000) U.S. consumers whom Defendant has identified whose Personal Information was accessed without authorization as a result of the Breach.

2. "**Alternative Reimbursement Compensation**" means compensation for any Affected Consumer who does not make a claim to enroll in the Product, and instead, has or has concurrent with their claim obtained a credit monitoring or protection product.

3. "**Assisted Identity Restoration Services**" means the identity restoration services, as set forth in Section IX and described in Exhibit A, offered to all Affected Consumers who have or may have experienced identity theft or fraud.

4. "**Breach**" means the information security incident publicly disclosed by Defendant on or about September 7, 2017.

5. "**Claims Administration Protocol**" means the protocol that has been approved by a representative of the Commission and which will be submitted to and approved by the MDL Court, to implement the claims administration and Settlement process in the Multi-District Litigation.

6. "**Claims Forms**" are the forms that have been approved by a representative of the Commission and which will be submitted to and approved by the MDL Court, that Affected Consumers submit to the Settlement Administrator in paper or via the Settlement Website to make claims for Out-of-Pocket Losses, Alternative Reimbursement Compensation, the Product, and Single-Bureau Monitoring.

7. "**Class Action Effective Date**" means the first business day after the MDL Court enters final approval of the Settlement, and either:

   a. the time for appeal, petition, rehearing or other review has expired, or

   b. if one or more appeals, petitions, requests for rehearing or other reviews are filed regarding any issue with the Settlement, when

      i. the final approval order and judgment is affirmed without material change and the time for further appeals, petitions, requests for rehearing or other reviews has expired, or

      ii. all appeals, petitions, rehearings, or other reviews are dismissed or otherwise disposed of and the time for further appeals, petitions, requests for rehearing or other review has expired.

8. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

   a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("Triggering Representation") is made in only one means.

b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

c. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

e. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in a language in which the Triggering Representation appears.

f. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

g. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

h. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

9. "**Consumer Fund**" means the account established to provide restitution and redress to Affected Consumers as described in Sections VIII, IX and X, and which will be overseen by the MDL Court and which represents an undifferentiated portion of the consumer restitution fund as defined in the Settlement.

10. "**Consumer Report**" has the meaning provided in the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*, and any amendments thereto. As of the date of entry of this Order, "Consumer Report" is defined under the FCRA as any written, oral, or other communication of any information by a Consumer Reporting Agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

a. credit or insurance to be used primarily for personal, family, or household purposes;

b. employment purposes; or

c. any other purpose authorized under FCRA Section 604, 15 U.S.C. § 1681b.

11. "**Consumer Reporting Agency**" has the meaning provided in the FCRA, 15 U.S.C. § 1681 *et seq.*, and any amendments thereto. As of the date of entry of this Order, "Consumer Reporting Agency" is defined under the FCRA as any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports.

12. "**Covered Incident**" means any instance in which any U.S. federal, state, or local law or regulation requires Defendant to notify any U.S. federal, state, or local government entity that Personal Information collected or received, directly or indirectly, by Defendant from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization, and the incident affects at least 250 U.S. consumers.

13. "**Defendant**" means (1) Equifax Inc., and its successors and assigns, and (2) Equifax Inc.'s subsidiaries, and their successors and assigns, incorporated in the United States, that do business in the United States, or that collect, store, or process Personal Information from or about consumers in the United States to the extent that their conduct falls within the Commission's jurisdiction.

14. "**Extended Claims Period**" means the period of time ending four years after the conclusion of the Initial Claims Period.

15. "**Full Service Identity Restoration Services**" means the identity restoration services offered to all Affected Consumers enrolled in the Product, as described in Exhibit A.

16. "**Initial Claims Period**" means the period of time ending six months after entry of the order permitting issuance of notice in the Multi-District Litigation.

17. "**MDL Court**" means the Court presiding over the Multi-District Litigation.

18. "**Multi-District Litigation**" means those actions filed against Equifax Inc. and/or one or more of its subsidiaries asserting claims related to the Breach by or on behalf of one or more consumers that have been or will be transferred to the federal proceedings styled *In re Equifax Inc. Customer Data Breach Litigation*, 1:17-md-02800-TWT (N.D. Ga.).

19. "**Notice and Settlement Administration Costs and Expenses**" means the costs and expenses of the Notice Provider, Notice Plan, Claims Administration Protocol, and Settlement Administrator.

20. "**Notice Date**" means sixty days after the MDL Court issues an order permitting issuance of notice of the Settlement.

21. "**Notice Plan**" means the plan that has been approved by a representative of the Commission and which will be submitted to, approved by, and overseen by the MDL Court, for providing notice to Affected Consumers in the Multi-District Litigation.

22. "**Notice Provider**" means Signal Interactive Media or another independent third-party agent or administrator that has been approved by a representative of the Commission, and which will be submitted to, approved by, and overseen by the MDL Court to implement the Notice Plan.

23. "**Out-of-Pocket Losses**" means verifiable unreimbursed costs or expenditures that an Affected Consumer incurred and that are fairly traceable to the Breach, which are eligible for reimbursement from the Consumer Fund as set forth in Sections IX.B.1.c and IX.B.2.

24. "**Personal Consumer Report**" means the Consumer Report made available to consumers by any entity within Defendant that compiles and maintains files on consumers on a nationwide basis as defined under 15 U.S.C. § 1681a(p).

25. "**Personal Information**" means individually identifiable information from or about an individual consumer, including:

    a. first and last name;

    b. home or other physical address;

    c. email address;

    d. telephone number;

    e. date of birth;

    f. Social Security number;

    g. other government-issued identification numbers, such as a driver's license number, military identification number, passport number, or other personal identification number;

    h. financial institution account number;

    i. credit or debit card information; or

    j. authentication credentials, such as a username and password.

26. "**Preventative Measures**" means placement or removal of security freezes or obtaining credit monitoring services.

27. "**Product**" means the three-bureau credit and identity monitoring product, including any changes, as described in Exhibit A and approved by a representative of the Commission and then approved by the MDL Court.

28. "**Service Awards**" means compensation awarded to the consumers named as plaintiffs in the Multi-District Litigation.

29. "**Settlement**" means the settlement resolving the Multi-District Litigation.

30. "**Settlement Administrator**" means JND Legal Administration, or another independent third-party agent or administrator that has been approved by a representative of the Commission, and which will be submitted to, approved by, and overseen by the MDL Court to implement the processes described in the Claims Administration Protocol, and claims and Settlement process in the Multi-District Litigation.

31. "**Settlement Website**" means the website established by the Settlement Administrator, and described in the Claims Administration Protocol, that has been approved by a representative of the Commission to provide information about the Settlement, including deadlines and case documents, and permit Affected Consumers to electronically submit Claims Forms.

32. "**States' Attorneys General**" means the 50 state and territory attorneys general that are each entering into a stipulated judgment on or about July 22, 2019 with Equifax Inc. for claims related to the Breach.

33. "**Time Compensation**" means compensation to an Affected Consumer for time spent by that Affected Consumer (1) taking Preventative Measures and/or (2) remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information that is fairly traceable to the Breach.

ORDER

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Defendant, Defendant's officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any good or service, are hereby permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Defendant maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information.

II. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Defendant shall establish and implement, and thereafter maintain, for twenty years after entry of this Order, a comprehensive information security program ("Information Security Program") designed to protect the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program, including the following:

1. Documented risk assessments required under Section II.D;

2. Documented safeguards required under Section II.E; and

3. A description of the procedures adopted to implement and monitor the Information Security Program, including procedures for evaluating and adjusting the Information Security Program as required under Section II.I;

B. Provide the written Information Security Program and any material evaluations thereof or updates thereto to Defendant's board of directors or a relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program at least once every twelve months;

C. Designate a qualified employee or employees to coordinate, oversee, and be responsible for the Information Security Program;

D. Assess, at least once every twelve months, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information and document those risks that are material. Defendant shall further assess and document internal and external risks as described above as they relate to a Covered Incident promptly (not to exceed forty-five days) following verification of such a Covered Incident;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Defendant identifies to the security, confidentiality, or integrity of Personal Information identified in response to Section II.D. Each safeguard shall be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood, given the existence of other safeguards, that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Such safeguards shall also include:

1. Establishing patch management policies and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated;

2. Establishing and enforcing policies and procedures to ensure the timely remediation of critical and/or high-risk security vulnerabilities;

3. Identifying and documenting a comprehensive information technology ("IT") asset inventory that includes hardware, software, and location of the assets;

4. Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring, across Defendant's network and IT assets, including Defendant's legacy technologies;

5. Designing, implementing, and maintaining measures to limit unauthorized access in any network or system that stores, collects, maintains, or processes Personal Information, such as segmentation of networks and databases and properly configured firewalls;

6. Implementing access controls across Defendant's network, such as multi-factor authentication and strong password requirements;

7. Limiting user access privileges to systems that provide access to Personal Information to employees, contractors, or other authorized third parties with a business need to access such information and establishing regular documented review of such access privileges;

8. Implementing protections, such as encryption, tokenization, or other at least equivalent protections, for Personal Information collected, maintained, processed, or stored by Defendant, including in transit and at rest. To the extent that any of the identified protections are infeasible, equivalent protections shall include effective alternative compensating controls designed to protect unencrypted data at rest or in transit, which shall be reviewed and approved by the qualified employee or employees designated to coordinate, oversee, and be responsible for the Information Security Program;

9. Establishing and enforcing written policies, procedures, guidelines, and standards designed to:

   a. Ensure the use of secure development practices for applications developed in-house; and

   b. Evaluate, assess, or test the security of externally developed applications used within Defendant's technology environment;

10. Establishing regular information security training programs, updated, as applicable, to address internal or external risks identified by Defendant, including, at a minimum:

   a. At least annual information security awareness training for all employees, including notifying employees of the process for submitting complaints and concerns pursuant to Section II.E.12; and

   b. Training for software developers relating to secure software development principles and intended to address well-known and reasonably foreseeable vulnerabilities, such as cross-site scripting, structured query language injection, and other risks identified by Defendant through risk assessments and/or penetration testing;

11. Establishing a clear and easily accessible process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics; and

12. By August 30, 2019, establishing a clear and easily accessible process overseen by a senior corporate manager for employees to submit complaints or concerns about Defendant's information security practices, including establishing a clear process for reviewing, addressing, and escalating employee complaints or concerns.

F. Assess, at least once every twelve months, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and evaluate and implement any needed modifications to the Information Security Program based on the results. Defendant shall further assess the sufficiency of safeguards as described above, as they relate to a Covered Incident, promptly (not to exceed forty-five days) following verification of such an incident. Each such assessment must evaluate safeguards in each area of relevant operation, including:

1. Employee training and management;

2. Information systems, such as network and software design, or information processing, storage, transmission, and disposal; and

3. Prevention, detection, and response to attacks, intrusions, or other system failures;

G. Test and monitor the effectiveness of the safeguards at least once every twelve months and, as they relate to a Covered Incident, promptly (not to exceed sixty days) following verification of such an incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of Defendant's network at least once every four months and, as it relates to a Covered Incident, promptly (not to exceed sixty days) following verification of such an incident, and penetration testing of Defendant's network at least once every twelve months and, as it relates to a Covered Incident, promptly (not to exceed sixty days) following verification of such an incident;

H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Defendant, and contractually require service providers to implement and maintain safeguards tailored to the amount and the type of Personal Information at issue; and

I. Evaluate and adjust the Information Security Program in light of any changes to Defendant's operations or business arrangements, including, without limitation, acquisition or licensing of any new information systems, technologies, or assets through merger or acquisition, a Covered Incident, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of the Information Security Program. At a minimum, Defendant must evaluate the Information Security Program at least once every twelve months and, as it relates to a Covered Incident, promptly (not to exceed sixty days) following verification of such an incident and modify the Information Security Program based on the results.

III. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Section II of this Order, titled Mandated Information Security Program, Defendant must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) is a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or other similarly qualified person or organization;

(3) has at least five years of experience evaluating the effectiveness of computer system security or information system security; (4) conducts an independent review of the Information Security Program; and (5) is contractually required to retain all documents relevant to each Assessment for five years after completion of such Assessment, and to provide such documents to the Commission within fourteen days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of (1) a claim of confidentiality, proprietary or trade secrets, or any similar claim, or (2) any privilege asserted between Defendant and the Assessor, although such documents can be designated for confidential treatment in accordance with applicable law.

B. For each Assessment, Defendant shall provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion. If the Associate Director for Enforcement does not approve of the person Defendant has selected, Defendant must choose a person or entity to conduct the Assessment from a list of at least three Assessors provided by a representative of the Commission.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the entry date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty years after entry of the Order for the biennial Assessments.

D. Each Assessment must:

1. Evaluate whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program;

2. Assess the effectiveness of Defendant's implementation and maintenance of subsections A-I of Section II;

3. Identify gaps or weaknesses in the Information Security Program and make recommendations to remediate or cure any such gaps and weaknesses; and

4. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Defendant's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by Defendant's management.

E. Each Assessment must be completed within sixty days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit each Assessment to the Commission within ten days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203." Defendant must notify the Commission of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Commission's procedures concerning public disclosure set forth in 15 U.S.C. 46(f) and 16 CFR 4.10.

IV. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any Assessment required by Section III of this Order titled Information Security Assessments by a Third Party, must not withhold any material facts from the Assessor, and must not misrepresent, expressly or by implication, any fact material to the Assessor's: (1) evaluation of whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of subsections A-I of Section II; or (3) identification of any gaps or weaknesses in the Information Security Program. Defendant shall provide the Assessor with information about Defendant's entire network and all of Defendant's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network and IT assets deemed in scope. Defendant shall also provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment.

V. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that, in connection with compliance with Section II of this Order titled Mandated Information Security Program, Defendant shall:

A. For a total of twenty years and commencing one year after the entry date of this Order, and each year thereafter, provide the Commission with a certification from the board of directors, or a relevant subcommittee thereof, or other equivalent governing body or, if no such board or equivalent governing body exists, a senior officer of Defendant responsible for Defendant's Information Security Program, that: (1) Defendant has established, implemented, and maintained the requirements of this Order; (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; (3) Defendant has cooperated with the Assessor as required by Section IV of this Order; and (4) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the board of directors, or relevant subcommittee thereof, or other equivalent governing body, reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

VI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that for twenty years from the entry of the Order, Defendant, within a reasonable time after the date of Defendant's discovery of a Covered Incident, but in any event no later than ten days after the date Defendant first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Commission.

A. The report must include, to the extent possible:

1. The date, estimated date, or estimated date range when the Covered Incident occurred;

2. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

3. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

4. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

5. The acts that Defendant has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and, if applicable, to protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

6. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Defendant to consumers or to any U.S. federal, state, or local government entity.

B. No more than thirty days after every calendar quarter, Defendant must provide Defendant's board of directors or a relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program, a report summarizing all Covered Incidents that occurred in that calendar quarter.

C. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., File No. 172 3203." Defendant must notify the Commission of any portions of the Covered Incident Report containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Commission's procedures concerning public disclosure set forth in 15 U.S.C. § 46(f) and 16 CFR Part 4.10.

VII. MONETARY JUDGMENT AND ADDITIONAL MONETARY OBLIGATIONS

IT IS FURTHER ORDERED that:

A. Judgment in the amount of Four Hundred Twenty-Five Million Dollars ($425,000,000) is entered in favor of the Commission against Defendant.

B. This order imposes additional financial obligations ("Additional Financial Obligations") on Defendant for the purpose of monetary relief for Affected Consumers. If more than seven million Affected Consumers enroll in the Product, then Defendant's Additional Financial Obligations will be calculated using the following formulas:

1. If, at the end of the Initial Claims Period, more than seven million Affected Consumers enroll in the Product, then:

a. If the total payments for Alternative Reimbursement Compensation, Out-of-Pocket Losses, Assisted Identity Restoration Services, Notice and Settlement Administration Costs and Expenses, Service Awards, and the cost of providing the Product to seven million Affected Consumers (the "Costs") are greater than or equal to Three Hundred Million Dollars ($300,000,000), Equifax Inc., its successors and assigns, shall pay the Commission an amount equal to the cost of providing the Product to enrollees above seven million (the "Additional Credit Monitoring Cost");

b. If the Costs are less than Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000) and the Additional Credit Monitoring Cost is greater than Forty-Three Million Five Hundred Thousand Dollars ($43,500,000), Equifax Inc., its successors and assigns, shall pay the Commission an amount equal to the Additional Credit Monitoring Cost less Forty-Three Million Five Hundred Thousand Dollars ($43,500,000); or

c. If (i) the Costs are greater than or equal to Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000) but less than Three Hundred Million Dollars ($300,000,000) and (ii) the Costs plus the Additional Credit Monitoring Costs are greater than Three Hundred Million Dollars ($300,000,000), Equifax Inc., its successors and assigns, shall pay the Commission an amount equal to the Costs plus Additional Credit Monitoring Costs less Three Hundred Million Dollars ($300,000,000); and

2. If, during the Extended Claims Period, more than seven million Affected Consumers have enrolled in the Product and either (i) the Costs are greater than or equal to Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000)or (ii) the Additional Credit Monitoring Costs are greater than or equal to Forty-Three Million Five Hundred Thousand Dollars ($43,500,000) then, on a monthly basis, Equifax Inc., its successors and assigns, shall deposit any additional money to the Commission that would be required pursuant to the calculations in Section VII.B.1.a-c, less any amounts previously deposited as the Additional Financial Obligations.

VIII. CONSUMER RESTITUTION AND REDRESS THROUGH MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED that consumer relief that would otherwise be conducted by the Commission using the monetary relief in Section VII may be instead conducted through final resolution of the Multi-District Litigation consistent with Sections VIII, IX, and X of this Order, beginning with filing an executed Settlement agreement and motion for entry of an order permitting issuance of notice of the Settlement containing each of the following components:

A. Equifax Inc., its successors and assigns, shall deposit Three Hundred Million Dollars ($300,000,000) (the "Payment") into the Consumer Fund as follows: (i) One Hundred Fifty Thousand Dollars ($150,000) no later than fifteen days after the filing of this Order, to cover reasonable set-up costs of the Notice Provider; (ii) Twenty-Five Million Dollars ($25,000,000) no later than fifteen days after the MDL Court enters an order permitting issuance of notice of the Settlement, to cover reasonable costs and expenses of the Settlement Administrator and Notice Provider and set-up costs for the independent third-party provider of the Product and Assisted Identity Restoration Services; and (iii) Three Hundred Million Dollars ($300,000,000) into the Consumer Fund, less any amounts paid pursuant to (i) and (ii), no later than fifteen days after the Class Action Effective Date.

B. If the Consumer Fund lacks sufficient funds to pay claims for Out-of-Pocket Losses made during the Initial and Extended Claims Periods, Equifax Inc., its successors and assigns, deposits into the Consumer Fund, as needed to pay such claims on a monthly basis, up to an additional aggregate amount of One Hundred Twenty-Five Million Dollars ($125,000,000) within fourteen days after receipt of written notification from the Settlement Administrator that there are insufficient funds remaining in the Consumer Fund.

C. Equifax Inc., its successors and assigns, pays any Additional Financial Obligations required under Section VII into the Consumer Fund.

D. Sections IX and X of this Order shall be construed in a manner consistent with the Settlement.

IX. CONSUMER FUND FOR MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED that:

A. An amount no less than Three Hundred Million Dollars ($300,000,000), plus any amount deposited in the Consumer Fund pursuant to Sections VIII.B and VIII.C, including all accumulated interest, must be used and administered as described in Section IX for the exclusive purpose of providing restitution and redress to Affected Consumers.

B. Subject to Sections IX.C and IX.D, the Consumer Fund shall be used to pay:

1. After either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later, for claims submitted during the Initial Claims Period:

a. Four years of enrollment in the Product to Affected Consumers, which shall include One Million Dollars ($1,000,000) in identity theft insurance and Full Service Identity Restoration Services.

i. The Product shall be offered, provided and maintained by an independent third party and shall not be provided to any Affected Consumer by Defendant. Defendant shall not receive any monetary benefit from the Product;

ii. Defendant shall, through the independent third party provider of the Product, provide activation codes for enrollment in the Product to Affected Consumers who file a valid claim for the Product. Activation codes shall be sent no later than forty-five days after either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later. Affected Consumers shall be eligible to enroll in the Product for a period of at least ninety days following receipt of the activation code.

b. Alternative Reimbursement Compensation of up to One Hundred Twenty-Five Dollars ($125);

c. Claims for Out-of-Pocket Losses, including, without limitation, the following:

i. Up to twenty-five percent (25%) reimbursement for costs incurred by an Affected Consumer enrolled in an Equifax credit or identity monitoring subscription product on or after September 7, 2016, through September 7, 2017;

ii. Credit monitoring costs that were incurred by an Affected Consumer on or after September 7, 2017, through the date of the Affected Consumer's claim submission;

iii. Costs incurred on or after September 7, 2017, associated with placing or removing a security freeze on a Consumer Report with any Consumer Reporting Agency;

iv. Unreimbursed costs, expenses, losses, or charges incurred by an Affected Consumer as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of Affected Consumers' personal information;

v. Other miscellaneous expenses incurred related to any Out-Of-Pocket Loss such as notary, fax, postage, copying, mileage, and long-distance telephone charges; and

vi. Time Compensation for up to twenty hours.

2. For claims submitted during the Extended Claims Period, reimbursement of claims for the following Out-of-Pocket Losses incurred during the Extended Claims Period:

a. Unreimbursed costs, expenses, losses, or charges incurred by an Affected Consumer as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of Affected Consumers' Personal Information;

b. Other miscellaneous expenses, incurred by an Affected Consumer related to remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information, such as notary, fax, postage, copying, mileage, and long-distance telephone charges; and

c. Time Compensation limited to time spent remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information that is fairly traceable to the Breach.

3. For a period of seven years from the Class Action Effective Date, Assisted Identity Restoration Services to an Affected Consumer. Affected Consumers shall not be required to enroll in the Product to obtain Assisted Identity Restoration Services.

   a. The Assisted Identity Restoration Services shall be offered, provided and maintained by the independent third party that has been approved by a representative of the Commission and that will be presented to the MDL Court for its approval. Assisted Identity Restoration Services shall not be provided to any Affected Consumer by Defendant. Defendant shall not receive any monetary benefit from the Assisted Identity Restoration Services.

4. Notice and Settlement Administration Costs and Expenses;

5. Applicable taxes, duties, and similar charges due from the Consumer Fund to the extent that the principal is not reduced; and

6. Service Awards in an aggregate amount not to exceed Two Hundred Fifty Thousand Dollars ($250,000). To the extent the MDL Court approves Service Awards in excess of Two Hundred Fifty Thousand Dollars ($250,000), such amount shall not be paid from the funds deposited into the Consumer Fund pursuant to this Order and shall be paid solely by the Defendant.

C. Subject to Section IX.D, payments from the Consumer Fund shall be subject to the following limitations:

1. Each Affected Consumer will be eligible to receive a maximum aggregate reimbursement of Twenty Thousand Dollars ($20,000) for Out-of-Pocket Losses.

2. No more than Thirty-One Million Dollars ($31,000,000) shall be used to pay Alternative Reimbursement Compensation (the "Alternative Reimbursement Compensation Cap"). To the extent valid claims for Alternative Reimbursement Compensation exceed the Alternative Reimbursement Compensation Cap, then payments for valid Alternative Reimbursement Compensation claims shall be reduced on a *pro rata* basis.

3. No more than Thirty-One Million Dollars ($31,000,000) shall be paid as Time Compensation for valid Time Compensation claims made during the Initial Claims Period (the "Initial Time Compensation Cap"). To the extent valid claims for Time Compensation made during the Initial Claims Period exceed the Initial Time Compensation Cap, payments for such valid claims will be reduced on a *pro rata*

basis. Valid claims for Time Compensation made during the Extended Claims Period will be paid in the order they are received and approved at the same *pro rata* rate (if applicable) as valid Time Compensation claims made during the Initial Claims Period. No more than Thirty-Eight Million Dollars ($38,000,000) in the aggregate shall be paid as Time Compensation for valid claims made during both the Initial Claims Period and Extended Claims Period (the "Aggregate Time Compensation Cap"). At the conclusion of the Extended Claims Period, and following payment of valid claims made during the Extended Claims Period, Time Compensation claims may be subject to Section IX.D, if applicable, in which case all valid Time Compensation claims will be paid at the same *pro rata* rate.

D. If amounts remain in the Consumer Fund at the conclusion of the Extended Claims Period, the remaining funds shall be distributed to provide restitution and redress as follows:

1. First, the Aggregate Time Compensation Cap and Alternative Reimbursement Compensation Cap shall both be lifted (if applicable) and payments increased *pro rata* to Affected Consumers with valid claims up to the full amount of those claims; then,

2. Second, to provide Assisted Identity Restoration Services to all Affected Consumers for up to an additional thirty-six months; then,

3. Third, to extend the duration of the Product to Affected Consumers enrolled in the Product until the funds in the Consumer Fund are exhausted.

X. NOTICE AND CLAIMS IN MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED, if Defendant elects to deposit money in the Consumer Fund:

A. Defendant shall supply the Notice Provider with information in its possession, custody, or control, to the extent reasonably available, regarding Affected Consumers sufficient to enable the Notice Provider to implement the Notice Plan.

B. Defendant shall supply the Settlement Administrator with information in its possession, custody, or control, to the extent reasonably available, regarding Affected Consumers sufficient to enable the Settlement Administrator to implement the Claims Administration Protocol. This shall include providing the Settlement Administrator with sufficient information to identify consumers who are eligible for reimbursement pursuant to IX.B.1.c.i, as those consumers are not required to submit supporting documentation for this type of Out-of-Pocket Loss.

C. Defendant must notify a designated representative of the Commission of any requested modifications to the Notice Plan or Claims Administration Protocol, including any change of the Notice Provider or Settlement Administrator, and any such modification requested by the Defendant must be approved by a designated representative of the Commission, with such approval not unreasonably withheld, and shall also require approval from the MDL Court.

D. In connection with the administration of the Consumer Fund overseen by the MDL Court:

1. The Commission may send a request for information regarding compliance with Sections VII – X of this Order to the Notice Provider and/or Settlement Administrator, and any request will include all parties to the Settlement and the Bureau. Discussion and fulfillment of responses to a request from the Commission shall be made consistent with the Claims Administration Protocol;

2. Defendant shall provide to the Commission the weekly reports prepared by the Settlement Administrator pursuant to the Multi-District Litigation that summarize information related to the claims administration; and

3. Defendant shall provide to the Commission copies of any information requested by and submitted to the Bureau.

Any information submitted to the Commission pursuant to this Section shall be treated as confidential until the Class Action Effective Date.

E. From the beginning of the Initial Claims Period until the Consumer Fund is exhausted, Defendant shall provide a representative of the Commission, on an annual basis, with the following information for the prior year:

1. A summary by month of the total number of claims submitted to the Settlement Administrator, the total dollar amount of claims submitted to the Settlement Administrator, the total number of claims paid by the Settlement Administrator, the total amount of claims paid by the Settlement Administrator, and the total amount of claim payments negotiated.

2. Regarding the Product and Assisted Identity Restoration Services outlined in Exhibit A, the following information:

a. The number of Affected Consumers who enrolled in the Product;

b. The number and total dollar amount of claims filed by Affected Consumers under the identity theft insurance provided pursuant to the Product and what percentage of those claims were paid;

c. The number of Affected Consumers who availed themselves of Full Service Identity Restoration Services in the year preceding the publication of the annual report; and

d. The number of Affected Consumers who availed themselves of Assisted Identity Restoration Services in the year preceding the publication of the annual report.

3. Information regarding notice, including the number of viewers who opened emails sent pursuant to the Notice Plan, the number of unique visitors to the Settlement Website, and the number of unique visitors who arrived from a hyperlink to the Settlement Website posted on or in each of the following:

a. www.equifax.com;

b. www.equifaxsecurity2017.com;

c. Defendant's Twitter notifications referenced in Section XV.A.4;

d. Defendant's Facebook notifications referenced in Section XV.A.5; and

e. The emails sent pursuant to the Notice Plan.

4. Regarding consumer complaints:

   a. The number of unique consumer complaints received by the Settlement Administrator or the third party providing the Product regarding:

      i. Access to the Settlement Website;

      ii. Enrollment in the Product;

      iii. Any of the Product components, including identity theft insurance;

      iv. Any other consumer rights to obtain relief under this Order; or

      v. Identity theft; and

   b. Defendant shall develop and implement a process to direct consumers that contact Defendant with issues related to the Settlement or the Consumer Fund to the Settlement Administrator and/or the Settlement Website.

5. The reporting period must cover: (1) the first year after the entry date of the order permitting issuance of notice of the Settlement; and (2) each year thereafter until the Consumer Fund has been exhausted.

6. This information must be submitted to the Commission within sixty days after the reporting period has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

7. Defendant shall transmit the information required pursuant to Section X.D without alteration and shall disclose any fact material to the information submitted. No information may be withheld on the basis of (1) a claim of confidentiality, proprietary or trade secrets, or any similar claim, or (2) any privilege asserted between Defendant and the Settlement Administrator, although such documents can be designated for confidential treatment in accordance with applicable law.

8. The information described in Section X.D shall be treated as confidential until the Class Action Effective Date. Defendant shall not object to publication of this information by the Commission, to the extent that such publication occurs after the Class Action Effective Date.

XI. REVERSION OF CONSUMER RELIEF TO ADMINISTRATION BY COMMISSION

IT IS FURTHER ORDERED that the Commission may end its forbearance of the collection of the judgment and use the procedures set forth in this Section, rather than through the Multi-District Litigation in Section VIII, and receive Defendant's payments directly as follows:

A. The forbearance will terminate upon written notice to Defendant upon the occurrence of one or more Termination Events. If any of the following Termination Events should occur, a representative of the Commission and the Bureau may, in their sole discretion, jointly send Defendant a written notice of a Termination Event:

1. An executed Settlement agreement, and a motion for an order permitting issuance of notice of the Settlement, containing terms materially similar to those outlined in Sections VIII, IX, X, and XIII and Exhibit A of this Order, are not submitted to the MDL Court within fourteen days after the filing of this proposed Order, provided however that the Defendant, Commission, or the Bureau are not the cause of such failure;

2. The MDL Court declines to enter an order permitting issuance of notice of the Settlement and either (i) a modified Settlement agreement is not submitted to the MDL Court within sixty days or (ii) a modified Settlement agreement is submitted to the MDL Court without Defendant first obtaining written approval from a representative of the Commission;

3. The MDL Court enters a final approval of a Settlement agreement in the Multi-District Litigation with terms that are materially different from the terms in Sections VIII-X and Exhibit A of this Order and Defendant has not obtained written approval from a representative of the Commission;

4. The MDL Court declines to enter a final approval of a Settlement agreement in the Multi-District Litigation with terms materially similar to those outlined in Sections VIII, IX, X, and XIII and Exhibit B of this Order and (i) a modified Settlement agreement is not submitted to the MDL Court within sixty days, or (ii) a modified Settlement agreement is submitted to the MDL Court without Defendant first obtaining written approval from a representative of the Commission;

5. The MDL Court's Final Approval Order is overturned on appeal and either (i) a modified Settlement agreement in the Multi-District Litigation is not submitted to the MDL Court within sixty days or (ii) a modified Settlement agreement in the Multi-District Litigation is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Commission;

6. The MDL Court approves a Settlement agreement or modified Settlement agreement, other than one approved by the Commission, resolving the Multi-District Litigation that interferes in any way with the Commission's ability to enforce this Order; or

7. If at any time the Settlement is terminated by any party to the Multi-District Litigation.

Where approval is required by a representative of the Commission, such approval shall not be unreasonably withheld (e.g., if the proposed modification is no less favorable to Affected Consumers than the terms of this Order) and shall be timely provided.

B. If an event described in Sections XI.B.2 – 6 results from an objection from the Commission, Bureau, or the States' Attorneys General in the MDL Court to either (i) the Settlement or (ii) a modified Settlement agreement in the Multi-District Litigation, and such Settlement or modified Settlement agreement contains terms that are materially similar to Sections VIII, IX, X, and XIII and Exhibit A, such event shall not constitute a Termination Event.

C. If the Commission and the Bureau jointly send Defendant a written notice of a Termination Event, Section XI of this Order will not be construed in a way that interferes with the Multi-District Litigation.

D. If the forbearance ends, within twenty-one days of receipt of written notice of a Termination Event, Equifax Inc., its successors and assigns, is ordered to pay the following amounts, plus any interest accumulated, less any payments that have already been disbursed by the Settlement Administrator from the Consumer Fund; Defendant is not entitled to any offset or other deduction unless a representative of the Commission agrees in writing in advance:

1. Three Hundred Million Dollars ($300,000,000), plus any interest accumulated, less any payments that have already been disbursed by the Settlement Administrator from the Consumer Fund;

2. If the funds paid pursuant to Section XI.D.1 are insufficient to pay claims for Out-of-Pocket Losses made during the Initial and Extended Claims Periods, and subject to the monetary limits, if applicable, set forth in Sections IX.B, IX.C and IX.D, Equifax Inc., its successors and assigns, shall make additional payments of up to One Hundred Twenty-Five Million Dollars ($125,000,000) in the aggregate as needed on a monthly basis within fourteen days after receipt of written notification from a representative of the Commission that there are insufficient funds remaining; and

3. Additional Financial Obligations, subject to the monetary limits, if applicable, set forth in Section IX.B, IX.C and IX.D, pursuant to Section VII.B.

E. All payments to the Commission must be made by electronic fund transfer in accordance with instructions provided by a representative of the Commission.

F. The Notice Provider and Settlement Administrator's acceptance of funds shall constitute the Notice Provider and Settlement Administrator's agreement to consent to the jurisdiction of this Court.

G. In addition to payment, Defendant remains obligated to cooperate in the administration of consumer relief. If a representative of the Commission requests in writing any information related to consumer relief, Defendant must provide it, in the form prescribed by the Commission, within fourteen days. Defendant shall provide the Commission with:

1. Sufficient information to enable the Commission to efficiently administer consumer relief.

2. Sufficient information regarding any steps toward consumer notice, claims, and relief that has been provided pursuant to the Consumer Fund by the Notice Provider or the Settlement Administrator to enable the Commission to efficiently administer consumer relief.

H. The Commission may, at its sole discretion, continue to work with the Notice Provider and Settlement Administrator on behalf of itself, the Bureau, and the States' Attorneys General.

1. Whether the Commission elects to continue to retain them, the Notice Provider and the Settlement Administrator shall provide the Commission with sufficient information regarding any steps toward consumer notice, claims, and relief that has been provided pursuant to the Consumer Fund to enable the Commission to efficiently administer consumer relief.

2. If a representative of the Commission requests in writing any information related to consumer relief, Defendant shall require the Notice Provider and the Settlement Administrator to provide it, to the extent reasonably available, in the form prescribed by the Commission, within fourteen days.

I. All other provisions of this Order shall remain in full force and effect.

XII. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets.

B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.

C. The facts alleged in the Complaint establish all elements necessary to sustain an action by the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.

D. Defendant acknowledges that its Taxpayer Identification Number, which Defendant must submit to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

E. All money paid to the Commission shall be deposited into a fund administered by the Commission or its designee to be used for consumer relief, on behalf of the Commission, the Bureau, and States' Attorneys General, including the types of consumer relief enumerated in Section IX (such as enrollment in a credit monitoring product, out-of-pocket losses, time compensation, miscellaneous expenses, and identity theft restoration services), and any attendant expenses for the administration of any fund. If a

representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after consumer relief is completed under this subsection, the Commission may apply any remaining money for such other consumer relief (including consumer information remedies) as it determines to be reasonably related to Defendant's practices alleged in the Complaint. Any money not used for such consumer relief is to be deposited to the U.S. Treasury as disgorgement. All processes and protocols for the effective and efficient administration of the consumer relief are within the sole discretion of the Commission or its representatives and Defendant has no right to challenge any actions the Commission or its representatives may take pursuant to Section XII.E.

XIII. SINGLE-BUREAU MONITORING AND IDENTITY THEFT PROTECTION

IT IS FURTHER ORDERED that Defendant shall:

A. Offer a single-bureau monitoring service with the features described in Exhibit A ("Single-Bureau Monitoring) that has been approved by a representative of the Commission, to Affected Consumers who file a valid claim for Single-Bureau Monitoring and who enroll in the Product. Such Affected Consumers may enroll in the Single-Bureau Monitoring upon expiration of the Product, including any extensions thereof pursuant to Section IX, such that the aggregate number of years of credit monitoring provided under Section IX and the Single-Bureau Monitoring equals ten years, except as described in Subsection XIII.B, below.

B. Offer Affected Consumers who were under the age of eighteen on May 13, 2017, additional years of Single-Bureau Monitoring such that the aggregate number of years of credit monitoring provided under Section IX and the Single-Bureau Monitoring equals eighteen years. If an Affected Consumer who enrolled in the Product is under the age of eighteen when the Product expires, the Single-Bureau Monitoring offered will be child monitoring services until such Affected Consumer reaches eighteen years of age.

C. Provide all Affected Consumers with an easily accessible process to place or remove security freezes or locks on their Personal Consumer Report for free for a period of ten years following the date of entry of this Order. Defendant shall not dissuade Affected Consumers from placing or choosing to place a security freeze. Should Defendant offer any standalone product or service as an alternative with substantially similar features as a security freeze (e.g., Lock & Alert), Defendant shall not seek to persuade Affected Consumers to choose the alternative product or service instead of a security freeze.

D. Separate and apart from any statutory or other legal requirements, for a period of seven years starting December 31, 2019, provide to all U.S. consumers a clearly accessible process to obtain six free copies during any twelve-month period of their Personal Consumer Report.

XIV. PROHIBITION ON ADVERTISING OR MARKETING TO CONSUMERS WHO USE IDENTITY THEFT PROTECTION SERVICES

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, shall not use any information provided by an Affected Consumer to enroll in or to use the products and services set forth in Sections IX, XIII.D, and Exhibit A, including the Product, Full Service Identity Restoration Services, Assisted Identity Restoration Services, and the Single-Bureau Credit Monitoring, or the free credit monitoring products (Equifax TrustedID Premier, Equifax Credit Watch Gold with 3 in 1 Monitoring, or Experian IDNotify) offered or paid by Defendant in connection with the Breach (or the fact that the consumer provided such information), to sell, upsell, cross-sell, or directly market or advertise its products or services unless Defendant:

A. Makes a Clear and Conspicuous disclosure, separate and apart from any "End User License Agreement," "Privacy Policy," "Terms of Use" page, describing how Defendant will use the Affected Consumer's information; and

B. Obtains and documents the Affected Consumer's affirmative express consent.

XV. ADDITIONAL NOTICE

IT IS FURTHER ORDERED that Defendant shall provide the following notices:

A. To Affected Consumers within seven days of entry of an order permitting issuance of notice of the Settlement, or the Commission notifying Defendant that it is exercising its rights under a Termination Event, whichever is earlier:

1. Posting a Clear and Conspicuous hyperlink to the Settlement Website on the top portion of the landing page for Defendant's primary, consumer-facing website, www.equifax.com, which shall state "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," which shall remain posted until the expiration of the Initial Claims Period;

2. Posting a Clear and Conspicuous hyperlink to the Settlement Website on the top portion for the landing page for Defendant's www.equifaxsecurity2017.com website, which shall state "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," which shall remain posted until the expiration of the Extended Claims Period;

3. Issuing a press release, using terms consistent with the approved Notice Plan, including a hyperlink to the Settlement Website, with information about the Product, the Consumer Fund, and the Settlement Website;

4. Sending a Twitter notification via Defendant's primary Twitter account monthly during the Initial Claims Period and then biannually during the Extended Claims Period, the text of which shall read "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement"; and

5. Posting a Facebook notification via Defendant's primary account monthly during the Initial Claims Period and then biannually during the Extended Claims Period, the text of which shall read "Visit [hyperlink to the Settlement website] for information on the Equifax Data Breach Settlement."

B. To U.S. consumers, issuing a press release seven days after the relief described in Section XIII.D becomes available, with information about the availability of six free copies of a U.S. consumer's Personal Consumer Report during any twelve-month period for seven years, including a hyperlink to the webpage where consumers can request free Personal Consumer Reports.

XVI. RULE VIOLATIONS

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from violating any provision of the Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314, a copy of which is attached hereto as Exhibit B.

XVII. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this Order:

A. Defendant, within seven days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten years after entry of this Order, Defendant must deliver a copy of this Order to: (a) all principals, officers, directors, and LLC managers and members; (b) all employees, agents, and representatives having managerial or supervisory responsibilities for conduct related to the subject matter of the Order; and (c) any business entity resulting from any change in structure as set forth in the Section titled Compliance Reporting; and

C. Delivery must occur within 7 days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

D. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XVIII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendant make timely submissions to the Commission:

A. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury in which Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Defendant; (b) identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the types of goods or services offered, the means of advertising,

marketing, and sales, and the categories or types of Personal Information collected, transferred, maintained, processed or stored by each business; (d) describe in detail whether and how Defendant is in compliance with each Section of this Order; and (e) provide a copy of or record proving each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 20 years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against the Defendant within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

XIX. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for 20 years after entry of the Order, and retain each such record for 5 years. Specifically, Defendant must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reasons for termination;

C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. A copy of each information security assessment required by this Order and any material evaluations of Defendant's physical, technical, or administrative controls to protect the confidentiality, integrity, or availability of Personal Information;

E. A copy of each widely disseminated and unique representation by Defendant that describes the extent to which Defendant maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information;

F. For five years after the date of preparation of each Assessment required by this Order, all materials and evidence that are in the Defendant's possession and control that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Defendant, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Defendant's compliance with related Sections of this Order, for the compliance period covered by such Assessment; and

G. All records necessary to demonstrate full compliance with each provision of this Order; including all submissions to the Commission.

XX. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant's compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission is authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission to interview any employee or other person affiliated with Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission may use all other lawful means, including posing, through its representatives as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XXI. SEVERABILITY

IT IS FURTHER ORDERED that if any clause, provision, or section of this Order shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Order and this Order shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XXII. RETENTION OF JURISDICTION

IT IS FUTHER ORDERED that this Court retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this _____ day of _____, _____.

United States District Judge

FOR PLAINTIFF FEDERAL TRADE COMMISSION:

/s/ Jacqueline K. Connor

JACQUELINE K. CONNOR
TIFFANY GEORGE
CATHLIN TULLY
Federal Trade Commission
600 Pennsylvania Ave. N.W.,
CC-8232
Washington, D.C. 20580
Telephone: (202) 326-2844
Facsimile: (202) 656-3062
E-mail(s): jconnor@ftc.gov
tgeorge@ftc.gov
ctully@ftc.gov

ANNA M. BURNS
GA Bar No. 558234
Federal Trade Commission
Southeast Region
225 Peachtree Street, N.E., Suite 1500
Atlanta, GA 30303
Telephone: (404) 656-1350
Facsimile: (404) 656-1379
E-mail: aburns@ftc.gov

Date: 07/19/2019

FOR DEFENDANT EQUIFAX INC:

/s/ John J. Kelley III
JOHN J. KELLEY III
Corporate Vice President, Chief Legal Officer
Equifax Inc.
1550 Peachtree Street, NW
Atlanta, GA 30309

Date: 7/19/19

/s/ Edith Ramirez
EDITH RAMIREZ
HARRIET PEARSON
MICHELLE KISLOFF
TIMOTHY TOBIN
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20024
Tel: (202) 637-5600
Fax: (202) 637-5910

Date: 7/19/19

EX-10.3 4 d734596dex103.htm EX-10.3

Exhibit 10.3

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

BUREAU OF CONSUMER FINANCIAL PROTECTION,

Plaintiff,

v.

EQUIFAX INC.,

Defendant.

Civil Action Number:

[PROPOSED] STIPULATED ORDER FOR PERMANENT INJUNCTION AND MONETARY JUDGMENT

Plaintiff, the Bureau of Consumer Financial Protection ("Bureau"), has filed its Complaint for a permanent injunction, civil penalties, and other relief in this matter. The Bureau brought this action pursuant to Sections 1031(a), 1036(a)(1), and 1054 of the Consumer Financial Protection Act of 2010 ("CFPA"), 12 U.S.C. §§ 5531(a), 5536(a)(1), and 5564, and sought relief, including civil penalties, pursuant to Section 1055 of the CFPA, 12 U.S.C. § 5565(c). Defendant Equifax Inc. ("Defendant" or "Equifax") waived service of the summons and the Complaint. The Bureau and Defendant stipulate to entry of this Order for Permanent Injunction and Monetary Judgment ("Order") to resolve all claims in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint alleges claims for relief under Sections 1031(a) and 1036(a)(1) of the CFPA, 12 U.S.C. §§ 5531(a) and 5536(a)(1).
3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. For purposes of this Order, Defendant admits the facts necessary to establish jurisdiction over it and the subject matter of this action.
4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorneys' fees.
5. All parties waive all rights to appeal or otherwise challenge or contest the validity of this Order.
6. Entry of the Order is in the public interest.

DEFINITIONS

For purposes of this Order, the following definitions apply:

7. "Affected Consumer" means the approximately One Hundred Forty Seven Million (147,000,000) U.S. consumers whom Defendant has identified as having their Personal Information accessed without authorization as a result of the Breach.

8. "Assisted Identity Restoration" means the identity restoration services offered to all Affected Consumers, as set forth in Subsection VII.D and described in Exhibit A.

9. "Breach" means the information security incident publicly disclosed by Defendant on or about September 7, 2017.

10. "Claims Administration Protocol" means the protocol that has been approved by the Bureau, and which will be submitted to and approved by the MDL Court, to implement the claims administration process consistent with Sections VII, IX, X and XI of this Order and the Class Action Settlement.

11. "Class Action Settlement" means the settlement agreement, including release of settlement class member claims, filed in the Multi-District Litigation with the MDL Court.

12. "Class Action Effective Date" means the first business day after the MDL Court enters a Final Approval Order and Judgment, and either:

    a. the time for appeal, petition, rehearing or other review has expired, or

    b. if one or more appeals, petitions, requests for rehearing or other reviews are filed, when:

        i. the Final Approval Order and Judgment is affirmed without material change and the time for further appeals, petitions, requests for rehearing or other reviews has expired, or

        ii. all appeals, petitions, rehearings, or other reviews are dismissed or otherwise disposed of, no other appeals, petitions, rehearings, or other reviews are pending, and the time for further appeals, petitions, requests for rehearing or other reviews has expired.

13. "Consumer Fund" means the account established to provide restitution and redress to Affected Consumers, as described in Sections IX, X, and XI, which will be overseen by the MDL Court and which represents an undifferentiated portion of the consumer restitution fund as defined in the Class Action Settlement.

14. "Consumer Report" has the meaning provided in the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq*., and any amendments thereto. As of the date of this Order, "Consumer Report" is defined under the FCRA as any written, oral, or other communication of any information by a Consumer Reporting Agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

    a. credit or insurance to be used primarily for personal, family, or household purposes;

    b. employment purposes; or

    c. any other purpose authorized under the FCRA, Section 604, 15 U.S.C. § 1681b.

15. "Consumer Reporting Agency" has the meaning provided in the FCRA, 15 U.S.C. § 1681 *et seq*., and any amendments thereto. As of the date of this Order, "Consumer Reporting Agency" is defined under the FCRA as any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports.

16. "Covered Incident" means any instance in which any United States federal, state, or local law or regulation requires Defendant to notify any U.S. federal, state, or local government entity that Personal Information collected or received, directly or indirectly, by Defendant from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization, and the incident affects no fewer than 250 U.S. consumers.

17. "Defendant" means Equifax Inc., its successors and assigns, and its subsidiaries, their successors and assigns, incorporated in the United States, that do business in the United States, or that collect, store, or process Personal Information from or about consumers in the United States to the extent that Defendant's conduct falls within the Bureau's jurisdiction.

18. "Effective Date" means the date on which this Stipulated Order is issued.

19. "Enforcement Director" means the Assistant Director of the Office of Enforcement for the Bureau of Consumer Financial Protection, or her delegate.

20. "Extended Claims Period" means the period beginning with the conclusion of the Initial Claims Period through four (4) years after the conclusion of the Initial Claims Period.

21. "Final Approval Order and Judgment" means an order and judgment that the MDL Court enters finally approving settlement, including release of the settlement class member claims in the Multi-District Litigation.

22. "FTC Order" means the Stipulated Order entered in the matter styled as *Federal Trade Commission v. Equifax Inc.*, filed on or about July 22, 2019 in the Federal District Court for the Northern District of Georgia.

23. "Full Service Identity Restoration" means the identity restoration services offered to all Affected Consumers enrolled in the Product, as set forth in Subsection VII.A and described in Exhibit A.

24. "Initial Claims Period" means six (6) months after the MDL Court enters an order permitting issuance of notice of class action settlement for the Class Action Settlement.

25. "MDL Court" means the Court presiding over the Multi-District Litigation.

26. "Multi-District Litigation" means those actions filed against Equifax Inc. and/or one or more of its subsidiaries asserting claims related to the Breach by or on behalf of one or more consumers that have been or will be transferred to the federal proceedings styled *In re: Equifax Inc. Customer Data Security Breach Litigation*, 1:17-md-02800-TWT (N.D. Ga.).

27. "Notice Date" means the date sixty (60) days after the MDL Court issues an order permitting issuance of notice of class action settlement for the Class Action Settlement.

28. "Notice Plan" means the notice plan for providing notice to Affected Consumers which has been approved by a representative of the Bureau, and is to be submitted to, approved by, and overseen by the MDL Court.

29. "Notice Provider" means an independent third-party agent or administrator approved by a representative of the Bureau, and which is to be submitted to, approved by, and overseen by the MDL Court to implement the notice provisions of the Notice Plan, and as set forth in Section X.

30. "Out-of-Pocket Losses" means verifiable unreimbursed costs or expenditures incurred by an Affected Consumer that are fairly traceable (as described in the Claims Administration Protocol) to the Breach, which are eligible for reimbursement from the Consumer Fund as set forth in Subsection IX.B.4, and defined as follows:

    a. Costs incurred for credit monitoring services at any time between September 7, 2017 and the date of the Affected Consumer's claim(s) submission;

    b. Up to twenty-five percent (25%) reimbursement for costs incurred by an Affected Consumer enrolled in Equifax credit or identity monitoring subscription products at any time between September 7, 2016 and September 7, 2017;

    c. Costs incurred by an Affected Consumer to place or remove a security freeze on a Consumer Report with any Consumer Reporting Agency at any time on or after September 7, 2017;

    d. Unreimbursed costs, expenses, losses, or charges incurred as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of the Affected Consumer's Personal Information;

    e. Reimbursement for Time Compensation; and

    f. Miscellaneous expenses incurred by the Affected Consumer related to any Out-Of-Pocket Losses, such as notary, fax, postage, copying, mileage, and telephone charges.

31. "Personal Consumer Report" means, for purposes of this Order only, a Consumer Report made available to consumers by any entity within Defendant that compiles and maintains files on consumers on a nationwide basis as defined under 15 U.S.C. § 1681a(p).

32. "Personal Information" means individually identifiable information from or about an individual consumer, including:

a. first and last name;

b. home or other physical address;

c. email address;

d. telephone number;

e. date of birth;

f. Social Security number;

g. other government-issued identification numbers, such as a driver's license number, military identification number, passport number, or other personal identification number;

h. financial institution account number;

i. credit or debit card information; or

j. authentication credentials, such as a username and password.

33. "Preventative Measures" means placement or removal of security freezes or obtaining credit monitoring services.

34. "Product" means the credit monitoring, identity theft insurance, and identity restoration services further described in Subsection VII.A and on pages 1-4 of Exhibit A, that has been approved by the Bureau and will be presented to the MDL Court for approval.

35. "Related Consumer Action" means any private action by or on behalf of one or more consumers, or enforcement action by another governmental agency, entity, or representative, brought against Defendant based on substantially the same facts as described in the Complaint.

36. "Settlement Administrator" means an independent third-party agent or administrator that has been approved by the Bureau, which will be submitted to, approved by, and overseen by the MDL Court, and which will implement the claims and administration process in the Multi-District Litigation.

37. "Settlement Website" means the website established by the Settlement Administrator that provides information to Affected Consumers about their rights and options consistent with Sections VII, IX, X and XI of this Order, including the components of the Consumer Fund available to Affected Consumers, where and how Affected Consumers may submit claims during the Initial and Extended Claims Periods, and all deadlines for making such claims.

38. "Single Bureau Monitoring" means credit monitoring provided by Defendant and offered to all Affected Consumers enrolled in the Product, as set forth in Subsection VII.B and described in Exhibit A.

39. "States' Attorneys General" means the 50 state and territory attorneys general that are each entering into a stipulated judgment on or about July 22, 2019 with Equifax Inc. for claims related to the Breach.

40. "Time Compensation" means compensation to an Affected Consumer for a valid claim for time spent by that Affected Consumer (1) taking Preventative Measures and/or (2) remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information that is fairly traceable to the Breach.

ORDER

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Defendant, Defendant's officers, agents, employees, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and enjoined from misrepresenting, expressly or by implication, the extent to which Defendant maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information.

II. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Defendant shall establish and implement, and thereafter maintain, for twenty (20) years after entry of this Order, a comprehensive information security program ("Information Security Program") designed to protect the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, Defendant must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program, including the following:

1. Documented risk assessment required under Subsection II.D;

2. Documented safeguards required under Subsection II.E; and

3. A description of the procedures adopted to implement and monitor the Information Security Program, including procedures for evaluating and adjusting the Information Security Program as required under Subsection II.I.

B. Provide the written Information Security Program and any material evaluations thereof or updates thereto to Defendant's board of directors or a relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program at least once every twelve (12) months;

C. Designate a qualified employee or employees to coordinate, oversee, and be responsible for the Information Security Program;

D. Assess, at least once every twelve (12) months, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information and document those risks that are material. Defendant shall further assess and document internal and external risks as described above as they relate to a Covered Incident promptly (not to exceed forty-five days) following verification of such a Covered Incident;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Defendant identifies to the security, confidentiality, or integrity of Personal Information identified in response to Subsection D. Each safeguard shall be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood, given the existence of other safeguards, that the risk could be realized and result in the unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Such safeguards shall also include:

1. Establishing patch management policies and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated;

2. Establishing and enforcing policies and procedures to ensure the timely remediation of critical and/or high-risk security vulnerabilities;

3. Identifying and documenting a comprehensive information technology ("IT") asset inventory that includes hardware, software, and location of the assets;

4. Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring, across Defendant's network and IT assets, including Defendant's legacy technologies;

5. Designing, implementing, and maintaining measures to limit unauthorized access in any network or system that stores, collects, maintains, or processes Personal Information, such as segmentation of networks and databases and properly configured firewalls;

6. Implementing access controls across Defendant's network, such as multi-factor authentication and strong password requirements;

7. Limiting user access privileges to systems that provide access to Personal Information to employees, contractors, or other authorized third parties with a business need to access such information and establishing regular documented review of such access privileges;

8. Implementing protections, such as encryption, tokenization, or other at least equivalent protections, for Personal Information collected, maintained, processed, or stored by Defendant, including in transit and at rest. To the extent that any of the identified protections are infeasible, equivalent protections shall include effective alternative compensating controls designed to protect unencrypted data at rest or in transit, which shall be reviewed and approved by the qualified employee or employees designated to coordinate, oversee, and be responsible for the Information Security Program;

9. Establishing and enforcing written policies, procedures, guidelines, and standards designed to:

   a. Ensure the use of secure development practices for applications developed in-house; and

   b. Evaluate, assess, or test the security of externally developed applications used within Defendant's technology environment;

10. Establishing regular information security training programs, updated, as applicable, to address internal or external risks identified by Defendant, including, at a minimum:

   a. At least annual information security awareness training for all employees; and

   b. Training for software developers relating to secure software development principles and intended to address well-known and reasonably foreseeable vulnerabilities, such as cross-site scripting, structured query language injection, and other risks identified by Defendant through risk assessments and/or penetration testing;

11. Establishing a clear and easily accessible process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics; and

12. By August 30, 2019, establishing a clear and easily accessible process overseen by a senior corporate manager for employees to submit complaints or concerns about Defendant's information security practices, including establishing a clear process for reviewing, addressing, and escalating employee complaints or concerns.

F. Assess, at least once every twelve (12) months, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and evaluate and implement any needed modifications to the Information Security Program based on the results. Defendant shall further assess the sufficiency of safeguards as described above as they relate to a Covered Incident promptly (not to exceed forty-five days) following verification of such an incident. Each such assessment must evaluate safeguards in each area of relevant operation, including:

1. Employee training and management;

2. Information systems, such as network and software design, or information processing, storage, transmission, and disposal; and

3. Prevention, detection, and response to attacks, intrusions, or other system failures;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and, as they relate to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of Defendant's network at least once every four (4) months and, as it relates to a Covered Incident, promptly (not to exceed sixty (60) days) following verification of such an incident, and penetration testing of Defendant's network at least once every twelve (12) months and, as it relates to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident;

H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Defendant, and contractually require service providers to implement and maintain safeguards tailored to the amount and the type of Personal Information at issue; and

I. Evaluate and adjust the Information Security Program in light of any changes to Defendant's operations or business arrangements, including, without limitation, acquisition or licensing of any new information systems, technologies, or assets through merger or acquisition, a Covered Incident, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of the Information Security Program. At a minimum, Defendant must evaluate the Information Security Program at least once every twelve (12) months and, as it relates to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident and modify the Information Security Program based on the results.

III. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Section II of this Order, titled Mandated Information Security Program, Defendant must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) is a Certified Information Systems Security Professional ("CISSP") or a Certified Information Systems Auditor ("CISA"), or other similarly qualified person or organization; (3) has at least five (5) years of experience evaluating the effectiveness of computer system security or information system security; (4) conducts an independent review of the Information Security Program; and (5) is

contractually required to retain all documents relevant to each Assessment for five (5) years after completion of such Assessment, and to provide such documents to the Bureau within fourteen days of receipt of a written request from a representative of the Bureau. No documents may be withheld by the Assessor on the basis of (1) a claim of confidentiality, proprietary or trade secrets, or any similar claim, or (2) any privilege asserted between Defendant and Assessor, although such documents can be designated for confidential treatment in accordance with applicable law.

B. For each Assessment, Defendant shall provide the Enforcement Director with the name and affiliation of the person selected to conduct the Assessment, which the Bureau shall have the authority to approve in its sole discretion. If the Bureau does not approve of the person Defendant has selected, Defendant must choose a person or entity to conduct the Assessment from a list of at least three Assessors provided by a representative of the Bureau.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the entry date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after entry of the Order for the biennial Assessments.

D. Each Assessment must:

1. Evaluate whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program;

2. Assess the effectiveness of Defendant's implementation and maintenance of Subsections A-I of Section II;

3. Identify gaps or weaknesses in the Information Security Program and make recommendations to remediate or cure any such gaps and weaknesses; and

4. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Defendant's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by Defendant's management.

E. Each Assessment must be completed within sixty days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Bureau representative in writing, Defendant must submit each Assessment to the Bureau within ten days after the Assessment has been completed via secure email to Enforcement_Compliance@cfpb.gov or by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, "Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02." Defendant must notify the Bureau of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Bureau's procedures concerning public disclosure set forth in 12 U.S.C. § 5512(c)(6)(A) and 12 C.F.R. § 1070.20 (2018).

F. An Assessment required pursuant to this Section may be satisfied by an assessment conducted in connection with the FTC Order.

IV. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any Assessment required by Section III of this Order titled Information Security Assessments by a Third Party, must not withhold any material facts from the Assessor, and must not misrepresent, expressly or by implication, any fact material to the Assessor's: (1) evaluation of whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of subsections A-I of Section II; or (3) identification of any gaps or weaknesses in the Information Security Program. Defendant shall provide the Assessor with information about the Defendant's entire network and all of Defendant's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network and IT assets deemed in scope. Defendant shall also provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment.

V. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that, in connection with compliance with Section II of this Order titled Mandated Information Security Program, Defendant shall:

A. For a total of twenty (20) years and commencing one year after the entry date of this Order, and each year thereafter, provide the Bureau with a certification from the board of directors, or a relevant subcommittee thereof, or other equivalent governing body or, if no such board or equivalent governing body exists, a senior officer of Defendant responsible for Defendant's Information Security Program, that: (1) Defendant has established, implemented, and maintained the requirements of this Order; (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Bureau; (3) Defendant has cooperated with the Assessor as required by Section IV of this Order; and (4) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the board of directors, or relevant subcommittee thereof, or other equivalent governing body, reasonably relies in making the certification.

B. Unless otherwise directed by a Bureau representative in writing, submit all annual certifications to the Bureau pursuant to this Order via email to Enforcement_Compliance@cfpb.gov or by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, "Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02."

VI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that for twenty (20) years from the entry of the Order, Defendant, within a reasonable time after the date of Defendant's discovery of a Covered Incident, but in any event no later than ten days after the date Defendant first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Bureau.

A. The report must include, to the extent possible:

1. The date, estimated date, or estimated date range when the Covered Incident occurred;

2. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

3. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;

4. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;

5. The acts that Defendant has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and, if applicable, to protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

6. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Defendant to consumers or to any U.S. federal, state, or local government entity.

B. No more than thirty days after every calendar quarter, Defendant must provide Defendant's board of directors or relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program, a report summarizing all Covered Incidents that occurred in that calendar quarter.

C. Unless otherwise directed by a Bureau representative in writing, all Covered Incident reports to the Bureau pursuant to this Order must be emailed to the Bureau via secure email to Enforcement_Compliance@cfpb.gov or sent by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, "Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02." Defendant must notify the Bureau of any portions of the Covered Incident Report containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Bureau's procedures concerning public disclosure set forth in 12 U.S.C. § 5512(c)(6)(A) and 12 C.F.R. § 1070.20 (2018).

VII. CREDIT MONITORING AND IDENTITY THEFT PROTECTION

IT IS FURTHER ORDERED that,

A. Defendant must, through an independent third party that will be subject to appointment and oversight by the MDL Court, offer all Affected Consumers four (4) years of a free three-bureau credit monitoring and identity theft protection product, including $1 million in identity theft insurance and Full Service Identity Restoration, as described in the attached Exhibit A (the "Product").

1. The Product shall be offered, provided, and maintained by an independent third party, and shall not be directly provided to any Affected Consumer by Defendant, Defendant's successors or assigns, or any subsidiary, affiliate, or joint venture of Defendant. Defendant shall not receive any monetary benefit from the Product.

2. Affected Consumers may file a claim to enroll in the Product at any time during the Initial Claims Period, as described in the Claims Administration Protocol.

3. Defendant shall, through the independent third party provider of the Product, provide activation codes for enrollment in the Product to Affected Consumers who file a valid claim for the Product. Activation codes shall be sent no later than forty-five (45) days after either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later. An Affected Consumer shall be eligible to enroll in the Product for a period of at least ninety (90) days following receipt of an activation code.

4. To the extent the independent third party providing the Product assigns personal identification numbers (PINs) to Affected Consumers who made a claim to enroll in the Product, such PINs shall be randomized. As part of the enrollment process, Affected Consumers shall be authenticated using knowledge-based authentication questions, or other comparable authentication procedures. Authentication procedures shall be used any time an Affected Consumer requests a Consumer Report, if applicable, or to lock or unlock their Consumer Report through the Product.

5. As provided in Subsection XI.G.3, the period during which the Product shall be provided to Affected Consumers may be extended.

B. Defendant shall also offer Affected Consumers who file valid claims and enroll in the Product with a single-bureau credit monitoring service ("Single Bureau Monitoring"), as described in Exhibit A.

1. Defendant shall provide such Single Bureau Monitoring upon expiration of the Product, including any extensions thereof pursuant to Subsection XI.G.3, to Affected Consumers who enroll in the Product and file valid claims for Single Bureau Monitoring. Defendant shall provide Single Bureau Monitoring for the period of time necessary for the aggregate number of years of credit monitoring provided under Subsections VII.A, XI.G.3, and VII.B to equal ten (10) years.

2. Defendant shall offer Affected Consumers who were under the age of 18 as of May 13, 2017, additional years of Single Bureau Monitoring, as described in Exhibit A, necessary for the aggregate number of years of credit monitoring provided under Subsections VII.A, XI.G.3, and VII.B to equal eighteen (18) years.

C. For any Affected Consumer who does not make a claim to enroll in the Product and instead has or has concurrently obtained a credit monitoring or protection product, which he or she will have in place for a minimum of six (6) months, such Affected Consumer may receive One Hundred Twenty-Five Dollars ($125.00) in alternative compensation ("Alternative Reimbursement Compensation") by submitting a claim for Alternative Reimbursement Compensation, as set forth in the Claims Administration Protocol.

D. Defendant shall, through an independent third party that will be subject to appointment and oversight by the MDL Court, offer all Affected Consumers, regardless of whether they have enrolled in the Product, seven (7) years of free identity restoration services, with the features described in Exhibit A ("Assisted Identity Restoration").

1. Assisted Identity Restoration shall be offered, provided, and maintained by the independent third party that has been approved by a representative of the Bureau and that will be presented to the MDL Court for approval. Assisted Identity Restoration Services shall not be directly provided to any Affected Consumer by Defendant, Defendant's successors or assigns, or any subsidiary, affiliate, or joint venture of Defendant. Defendant shall not receive any monetary benefit from Assisted Identity Restoration.

2. Any Affected Consumer may avail himself or herself of the free Assisted Identity Restoration, as described in Exhibit A, for seven (7) years from the Class Action Effective Date regardless of whether that Affected Consumer filed a claim to enroll in the Product during the Initial Claims Period.

E. Defendant shall provide all consumers, regardless of whether they are Affected Consumers, with an easily accessible process to place or remove security freezes or locks on their Personal Consumer Reports for free and without filing a claim for ten (10) years from either (1) the Effective Date of this Order or (2) the Class Action Effective Date, whichever shall occur first.

1. Defendant shall randomize PINs to Affected Consumers requesting a Personal Consumer Report, or lock or security freeze of a Personal Consumer Report.

2. Defendant, and all other persons acting at Defendant's direction, shall not dissuade or seek to dissuade Affected Consumers from placing or choosing to place a security freeze. Should Defendant offer any standalone product or service as an alternative with substantially similar features as a security freeze, Defendant shall not seek to persuade Affected Consumers to choose the alternative product or service instead of a security freeze.

F. Defendant shall, for a period of seven (7) years beginning no later than December 31, 2019, provide to all U.S. consumers a clearly accessible process to obtain six (6) free copies during any 12-month period of their Personal Consumer Report, in addition to any free reports to which consumers are entitled under federal law, updated as of the time of request.

G. Defendant shall, for a period of ten (10) years from the Effective Date of this Order, develop and implement dispute handling procedures, including escalation to agents specially trained in fraud and a sufficient number of call center representatives to handle reasonably expected call volumes, for Affected Consumers who assert that information on their Personal Consumer Reports is inaccurate as a result of identity theft or fraud.

VIII. PROHIBITION ON ADVERTISING OR MARKETING TO CONSUMERS WHO USE IDENTITY PROTECTION SERVICES

IT IS FURTHER ORDERED that Defendant, Defendants' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, shall not use any information provided by Affected Consumers (or the fact that the consumer provided information) to enroll in or use, the Product, the Single Bureau Monitoring, the Full Service or Assisted Identity Restoration set forth in Section VII and Exhibit A, or the free credit monitoring products offered by Defendant in connection with the Breach—Equifax TrustedID Premier, Equifax Credit Watch Gold with 3 in 1 Monitoring, or Experian IDNotify—to sell, upsell, cross-sell, or directly market or advertise its products or services, unless Defendant first obtains and documents the consumer's affirmative express consent.

IX. CONSUMER FUND

IT IS FURTHER ORDERED that:

A. Equifax Inc., its successors and assigns, must deposit the amounts specified in Section XI.B below into the Consumer Fund for the purpose of providing restitution and redress to Affected Consumers, as required by this Section. All applicable taxes, duties, and similar charges due from the Consumer Fund shall be paid from the interest earned on the Consumer Fund.

B. Pursuant to Section XI, and as set forth in the Claims Administration Protocol, the Consumer Fund shall be used to pay or fund the following:

1. The cost of providing the Product, including Full Service Identity Restoration, as described in Subsection VII.A and Exhibit A, subject to the requirements of Subsection XI.E;

2. The cost of providing Assisted Identity Restoration, as described in Subsection VII.D and Exhibit A;

3. Reimbursements to Affected Consumers who file valid claims for Alternative Reimbursement Compensation, as described in Subsection VII.C;

4. Reimbursements to Affected Consumers who file valid claims for Out-of-Pocket Losses;

5. Costs and expenses of the Settlement Administrator, including but not limited to processing claims;

6. Costs and expenses of the Notice Provider, including but not limited to implementing and providing notice to Affected Consumers pursuant to the Notice Plan; and

7. Service awards, if any, to the Affected Consumers named as plaintiffs in the Multi-District Litigation in the amount approved by the MDL Court.

   a. Such service awards are not being ordered by the Bureau. Nonetheless, the Bureau does not object to up to Two Hundred Fifty Thousand Dollars ($250,000) from the Consumer Fund being used to pay service awards to the named plaintiffs in the Multi-District Litigation. To the extent the MDL Court approves service awards in excess of $250,000, such amounts shall not be paid from the funds deposited into the Consumer Fund pursuant to Section XI.B and shall be paid solely by the Defendant.

C. Subject to Subsection XI.G, payments from the Consumer Fund shall be subject to the following limitations:

1. Any Affected Consumer may request the restitution and redress described in this Section as follows:

a. During the Initial Claims Period, Affected Consumers may file claims for (1) the Product, (2) Single Bureau Monitoring, (3) Alternative Reimbursement Compensation, and (4) reimbursement of Out-of-Pocket Losses;

b. During the Extended Claims Period, Affected Consumers may file claims for reimbursement for the following Out-of-Pocket Losses incurred during the Extended Claims Period, only if the Affected Consumer provides a certification that he or she has not obtained reimbursement for the claimed expense through other means:

(i) Unreimbursed costs, expenses, losses, or charges incurred by an Affected Consumer as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of an Affected Consumer's Personal Information;

(ii) Time Compensation to an Affected Consumer, limited to time spent remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information that is fairly traceable to the Breach; and

(iii) Other miscellaneous expenses, incurred by an Affected Consumer related to remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information, such as notary, fax, postage, copying, mileage, and long-distance telephone charges.

2. An Affected Consumer may obtain up to an aggregate maximum amount of $20,000 in Out-of-Pocket Losses.

3. Time Compensation, a subcategory of Out-of-Pocket Losses, shall be subject to the following provisions:

a. Affected Consumers who spent or spend time (1) taking Preventative Measures or (2) remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach may seek reimbursement for their time.

b. Subject to Subsection IX.C.5, Time Compensation shall be paid at a rate of $25 per hour, reimbursable in 15-minute increments, with a minimum reimbursement of 1 hour per valid claim for Time Compensation.

c. Affected Consumers may submit a claim for up to 10 hours of Time Compensation, provided they certify (i) to taking Preventative Measures and/or remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach, and (ii) an explanation of the time they spent taking Preventative Measures or remedying fraud, identity theft, or other alleged misuse of their Personal Information.

d. Affected Consumers may submit a claim for up to 20 hours of Time Compensation, provided they spent time remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach, and provide (i) reasonable documentation (as defined in the Claims Administration Protocol) of the fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach and (ii) describe the time spent remedying these issues or time spent taking Preventative Measures in response to these issues.

4. No more than Thirty-One Million Dollars ($31,000,000) shall be paid as Alternative Reimbursement Compensation for valid claims filed during the Initial Claims Period (the "Alternative Reimbursement Compensation Cap"). To the extent valid claims for Alternative Reimbursement Compensation made during the Initial Claims Period exceed the Alternative Reimbursement Compensation Cap, payments for such valid claims shall be reduced on a *pro rata* basis. At the conclusion of the Extended Claims Period, after all payments required by Subsection IX.B have been made, if there are remaining unused funds in the Consumer Fund, the Alternative Reimbursement Compensation Cap shall be lifted, and payments to Affected Consumers who filed valid claims for Alternative Reimbursement Compensation shall be increased on a *pro rata* basis, up to the full amount of the valid claim, as set forth in Section XI.G.1 below.

5. No more than Thirty-One Million Dollars ($31,000,000) shall be paid as Time Compensation for valid Time Compensation claims made during the Initial Claims Period (the "Initial Time Compensation Cap"). To the extent valid claims for Time Compensation made during the Initial Claims Period exceed the Initial Time Compensation Cap, payments for such valid claims shall be reduced on a *pro rata* basis. Valid claims for Time Compensation made during the Extended Claims Period shall be paid in the order they are received and approved at the same *pro rata* rate (if applicable) as valid Time Compensation claims made during the Initial Claims Period. No more than Thirty-Eight Million Dollars ($38,000,000) in the aggregate shall be paid as Time Compensation for valid claims made during both the Initial Claims Period and Extended Claims Period ("Aggregate Time Compensation Cap"). At the conclusion of the Extended Claims Period, after payment of valid claims made during the Extended Claims Period, to the extent there are remaining unused funds in the Consumer Fund, the Aggregate Time Compensation Cap shall be lifted, and payments to all Affected Consumers who filed valid claims for Time Compensation shall be increased on a *pro rata* basis, up to the full amount of the valid claim, as set forth in Section XI.G.1 below.

X. NOTICE AND CLAIMS ADMINISTRATION

IT IS FURTHER ORDERED, that

A. The Notice Plan: Notice to Affected Consumers shall be provided pursuant to the Notice Plan. Defendant shall supply the Notice Provider with information in its possession, custody, or control, to the extent reasonably available, regarding the Affected Consumers to enable the Notice Provider to implement the Notice Plan.

B. The Claims Administration Protocol: Restitution and redress to Affected Consumers shall be administered from the Consumer Fund consistent with the Claims Administration Protocol. Defendant shall supply the Settlement Administrator with information in its possession, custody, or control, to the extent reasonably available, regarding the Affected Consumers to enable the Settlement Administrator to implement and administer the Claims Administration Protocol.

C. Defendant must notify the Bureau of any requested modifications to the Notice Plan or Claims Administration Protocol, including any change of the Notice Provider or Settlement Administrator, and any such modification requested by the Defendant must be approved by a designated representative of the Bureau, with such approval not unreasonably withheld, and shall also require approval from the MDL Court.

D. In connection with the administration of the Consumer Fund overseen by the MDL Court:

1. The Bureau may send a request for information regarding compliance with the Notice Plan, the claims process, and proper administration of the Consumer Fund, and any request will include all parties to the Class Action Settlement and the Commission. Discussion and fulfillment of responses to a request from the Bureau will be made consistent with the Claims Administration Protocol;

2. The Defendant shall provide to the Bureau the weekly reports prepared by the Settlement Administrator pursuant to the Multi-District Litigation that summarize information related to claims administration;

3. The Defendant shall provide to the Bureau copies of any reports submitted to the Federal Trade Commission under the FTC Order; and

4. The information provided to the Bureau described in this Section X.D shall be treated as confidential pursuant to 12 C.F.R. §1070 (2018) until at least the Class Action Effective Date.

E. Following the Class Action Effective Date, upon written request by the Bureau, Defendant shall provide the following information, if available, in accordance with instructions provided by a representative of the Bureau to Defendant.

1. The number of unique clicks on the hyperlink for the Settlement Website from the homepage of Defendant's primary, consumer-facing website, www.equifax.com;

2. The number of unique clicks on the hyperlink for the Settlement Website from Defendant's incident website, www.equifaxsecurity2017.com;

3. The number of viewers who reached the Settlement Website through the notice methods as described in the Notice Plan, where such information can be obtained, including via email communication;

4. The number of Affected Consumers who filed a claim to enroll in the Product;

5. The number of Affected Consumers who completed enrollment in the Product;

6. The number and total dollar amount of claims filed by Affected Consumers under the identity theft insurance provided pursuant to the Product, and the total dollar figure and percentage of claims paid;

7. The number of Affected Consumers who filed a claim to enroll in the Single Bureau Monitoring;

8. The number of Affected Consumers who completed enrollment in the Single Bureau Monitoring;

9. The number of Affected Consumers who availed themselves of the Full Service Identity Restoration and Assisted Identity Restoration;

10. The number of Affected Consumers who filed claims for Out-of-Pocket Losses; the total amounts claimed for each subcategory of Out-of-Pocket Losses; the total amount disbursed from the Consumer Fund for each subcategory of Out-of-Pocket Losses, and the average number of days between the date of the claim and the date of disbursement;

11. The number of Affected Consumers who filed claims for Alternative Reimbursement Compensation; the total dollar amount of claims filed for Alternative Reimbursement Compensation; the total amount disbursed from the Consumer Fund for Alternative Reimbursement Compensation; and the average number of days between the date of the claim and the date of disbursement;

12. The number of consumer complaints received by the Settlement Administrator or the third party providing the Product, regarding (a) access to the Settlement Website, (b) enrollment in the Product, (c) the Product components, (d) identity theft, and (e) other complaints received by the Settlement Administrator relating to the provision of restitution and redress through the Consumer Fund, including the claims process. Defendant shall develop and implement a process to direct consumers that contact Defendant with issues related to the Class Action Settlement or the Consumer Fund to the Settlement Administrator and/or the Settlement Website;

13. The number of consumers who file a dispute or appeal with the Settlement Administrator regarding a denial of any claim; the number of appeals denied; the number of appeals approved; the average number of days between the date of the appeal and the appeal decision; and the average number of days between the appeal decision and disbursement, if applicable; and

14. Any annual reports submitted to the Federal Trade Commission pursuant to the FTC Order.

F. Defendant shall also take the following additional measures to notify Affected Consumers of their ability to enroll in the Product and obtain the restitution and redress set forth in this Order using terms consistent with the approved Notice Plan by, no later than:

1. One day after filing of this Order:

a. Posting a hyperlink to the Settlement Website on the top portion of the landing page for Defendant's primary, consumer-facing website, www.equifax.com, which shall state "Visit www.EquifaxBreachSettlement.com for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," until the expiration of the Initial Claims Period; and

b. Posting a hyperlink to the Settlement Website on Defendant's incident website, www.equifaxsecurity2017.com, which shall state "Visit www.EquifaxBreachSettlement.com for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," until the expiration of the Extended Claims Period.

2. Seven (7) days of entry of an order permitting issuance of notice of the Class Action Settlement:

   a. Issuing a press release, including a hyperlink to www.EquifaxBreachSettlement.com with information about the Product, the Consumer Fund, and the Settlement Website;

   b. Posting a monthly Twitter notification via Defendant's primary Twitter account, the text of which shall read "Visit www.EquifaxBreachSettlement.com for information on the Equifax Data Breach Settlement" until the expiration of the Initial Claims Period, and biannually thereafter until the expiration of the Extended Claims Period; and

   c. Posting a monthly Facebook notification via Defendant's primary Facebook account, the text of which shall read "Visit www.EquifaxBreachSettlement.com for information on the Equifax Data Breach Settlement" until the expiration of the Initial Claims Period, and biannually thereafter until the expiration of the Extended Claims Period.

3. To U.S. Consumers, issuing a press release seven (7) days after the relief described in Section VII.F becomes available, with information about the availability of six free copies of a U.S. consumer's Personal Consumer Report during any twelve-month period for seven years, including a hyperlink to the webpage where consumers can request free Personal Consumer Reports.

XI. MONETARY JUDGMENT

IT IS FURTHER ORDERED that:

A. Judgment in the amount of Four Hundred Twenty-Five Million Dollars ($425,000,000) is entered in favor of the Bureau against Defendant for the purpose of providing restitution and redress to Affected Consumers.

B. Equifax Inc., its successors and assigns, shall pay this judgment as follows:

1. No later than fifteen (15) days following the date this Order is filed, Equifax Inc. shall deposit into the Consumer Fund One Hundred Fifty Thousand Dollars ($150,000) to cover reasonable set-up costs of the Notice Provider;

2. No later than fifteen (15) days after the MDL Court enters an order permitting issuance of notice of class action settlement for the Class Action Settlement, Equifax Inc., its successors and assigns, shall deposit into the Consumer Fund Twenty-Five Million Dollars ($25,000,000) to cover reasonable costs and expenses of the Settlement Administrator and Notice Provider and set-up costs for the independent third-party providing the Product and Assisted Identity Restoration;

3. No later than fifteen (15) days following the Class Action Effective Date, Equifax Inc., its successors and assigns, shall deposit Three Hundred Million Dollars ($300,000,000) into the Consumer Fund, less any amounts paid pursuant to Sections XI.B.1 and XI.B.2, to be used for the purposes set forth in Sections VII and IX; and

4. Equifax Inc., its successors and assigns, shall make all payments into the Consumer Fund as required by Section XI.C, up to a maximum of One Hundred Twenty-Five Million Dollars ($125,000,000).

C. If at any time during the Initial Claims Period or the Extended Claims Period, there are insufficient funds in the Consumer Fund (or, if it has received a written notice of a Triggering Event as described below in Subsection XI.I, a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and the States' Attorneys' General) to pay valid claims pursuant to Section IX (a "Shortfall"), Equifax Inc., its successors and assigns, shall make additional payments into the Consumer Fund of up to One Hundred Twenty-Five Million Dollars ($125,000,000) for the purpose of paying Out-of-Pocket Losses.

D. Defendant shall notify the Enforcement Director within three (3) business days of when the Settlement Administrator notifies Defendant of a Shortfall, as set forth in the Claims Administration Protocol. This notification shall identify the amount needed to pay the Shortfall. Within fourteen (14) days of receiving written notice from the Settlement Administrator of a Shortfall, Equifax Inc., its successors and assigns, shall deposit money into the Consumer Fund in the amount necessary to cure the Shortfall.

E. Equifax Inc., its successors and assigns, is ordered to pay into the Consumer Fund (or, if it has received a written notice of a Triggering Event as described below in Subsection XI.I, a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and the States' Attorneys' General) additional amounts for purposes of providing restitution and redress to Affected Consumers, as follows:

1. If, at the end of the Initial Claims Period, more than 7 million Affected Consumers have enrolled in the Product, the following obligations apply:

   a. If the total payments required under Subsections IX.B.2-7 and the cost of providing the Product to 7 million Affected Consumers (the "Costs") are greater than or equal to Three Hundred Million Dollars ($300,000,000), Equifax Inc., its successors and assigns, shall pay into the Consumer Fund an amount equal to the cost of providing the Product to enrollees above 7 million (the "Additional Credit Monitoring Cost");

   b. If the Costs are less than $256,500,000 and the Additional Credit Monitoring Cost is greater than $43,500,000, Equifax Inc., its successors and assigns, shall pay into the Consumer Fund an amount equal to the Additional Credit Monitoring Cost less $43,500,000; and

   c. If (i) the Costs are greater than or equal to $256,500,000, but less than $300,000,000 and (ii) the Costs plus the Additional Credit Monitoring Costs are greater than $300,000,000, Equifax Inc., its successors and assigns, shall pay into the Consumer Fund an amount equal to the Costs plus Additional Credit Monitoring Costs less $300,000,000.

2. If, during the Extended Claims Period, more than 7 million Affected Consumers have enrolled in the Product and either (i) the Costs are greater than or equal to $256,500,000 or (ii) the Additional Credit Monitoring Costs are greater than or equal to $43,500,000 then, on a monthly basis, Equifax Inc., its successors and assigns shall deposit any additional money into the Consumer Fund that would be required pursuant to the calculations in Subsection XI.E.1.a-c, less any amounts previously deposited pursuant to Subsection XI.E.1 or previously under this subsection.

F. An amount no less than $300 million, plus any amount deposited in the Consumer Fund pursuant to Subsections XI.C and XI.E, including all accumulated interest, must be used and administered as described in Subsections VII and IX for the exclusive benefit of Affected Consumers.

G. At the conclusion of the Extended Claims Period, the Settlement Administrator shall distribute or use any remaining funds as follows:

1. First, the Aggregate Time Compensation Cap and Alternative Reimbursement Compensation Cap, as described in Subsections IX.C.4-5, shall both be lifted (if applicable) and payments increased *pro rata* to Affected Consumers who submitted valid claims for Time Compensations and/or Alternative Reimbursement Compensation up to the full amounts of those claims; then

2. Second, to provide Assisted Identity Restoration to all Affected Consumers for up to an additional thirty-six (36) months in full-month increments; then

3. Third, to extend the duration of the Product to Affected Consumers enrolled in the Product until the funds in the Consumer Fund are exhausted.

H. The money deposited into the Consumer Fund and all accumulated interest shall be administered by the Settlement Administrator consistent with the Claims Administration Protocol.

I. If any of the following events ("Triggering Events") should occur, the Bureau and the Federal Trade Commission may, in their sole discretion, jointly send Defendant a written notice of a Triggering Event:

1. A settlement agreement releasing settlement class action member claims in the Multi-District Litigation and a motion for an order permitting issuance of notice of the Class Action Settlement containing terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order, is not submitted to the MDL Court within fourteen (14) days after the filing of this Order, provided however that the Defendant, the Bureau, or the Federal Trade Commission are not the cause of such failure;

2. The MDL Court declines to enter an order permitting issuance of notice of class action settlement for a settlement agreement releasing settlement class member claims in the Multi-District Litigation with terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided;

3. The MDL Court declines to enter a Final Approval Order for a settlement agreement releasing settlement class member claims in the Multi-District Litigation with terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided;

4. The MDL Court's Final Approval Order is overturned on appeal and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims in the Multi-District Litigation is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided; and

5. The MDL Court approves a modified settlement agreement other than the one approved by the Bureau releasing settlement class member claims in the Multi-District Litigation that interferes in any way with the Bureau's ability to enforce this Order.

J. If one of the events described in Subsection XI.I.2-4 occurs as a result of an objection filed by the Bureau, the Commission, or the States' Attorneys General in the MDL Court to either the Class Action Settlement or a modified settlement agreement releasing settlement class member claims in the Multi-District Litigation and such Class Action Settlement or modified settlement agreement contains terms materially similar to Sections VII, IX, X, and XI, and Exhibit A, such event shall not constitute a Triggering Event. If the Commission and the Bureau jointly send Defendant a written notice of a Triggering Event, Sections XI.I-L of this Order will not be construed in a way that interferes with the Multi-District Litigation.

K. Any modified settlement agreement submitted to the MDL Court pursuant to Subsections XI.I.2-4 shall contain terms that provide no less relief to Affected Consumers than set forth in this Order. If Defendant fails to comply with Subsections XI.B.1, XI.B.2, XI.B.3, or XI.B.4, and receives written notice of such failure, or if the Bureau and Federal Trade Commission send Defendant a written notice of a Triggering Event pursuant to XI.I, then the Bureau may move to enforce this Order. Defendant waives any objections to the Bureau's motion to enforce the Order under the circumstances described in this paragraph. All other provisions of this Order shall remain in full force and effect, and the Bureau and Commission shall jointly notify Defendant in writing that the Notice Plan (to the extent it has not already been administered) and the Claims Administration Protocol will be administered under the supervision of the Federal Trade Commission on behalf of the Bureau, the Federal Trade Commission, and the States' Attorneys General pursuant to Section XI of the FTC Order.

L. If Defendant fails to comply with Subsections XI.B.1, XI.B.2, XI.B.3, or XI.B.4, and receives a written notice of such failure, or Defendant receives a written notice of a Triggering Event as further described in Subsection XI.I, then Equifax Inc., its successors and assigns, shall pay the judgment as follows:

1. Within twenty one (21) days, deposit $300,000,000 plus any interest accumulated in the Consumer Fund attributed to any payment required pursuant to Section XI.B, less any payments that have already been disbursed by the Settlement Administrator, into a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and States' Attorneys' General to be used for consumer restitution and redress as set forth in this Order;

2. Make all payments required by Subsection XI.C up to a maximum of One Hundred Twenty-Five Million Dollars ($125,000,000) into such fund; and

3. Make all payments required by Subsection XI.E into such fund.

XII. CIVIL MONEY PENALTIES

IT IS FURTHER ORDERED that:

A. Under section 1055(c) of the CFPA, 12 U.S.C. § 5565(c), by reason of the violations of law described in the Complaint, and taking into account the factors in 12 U.S.C. § 5565(c)(3), Equifax Inc., its successors and assigns, must pay a civil money penalty of One Hundred Million Dollars ($100,000,000) to the Bureau ("Civil Money Penalty"). The penalty paid under this Order will be deposited in the Civil Penalty Fund of the Bureau as required by section 1017(d) of the CFPA, 12 U.S.C. § 5497(d).

B. Within 30 days of the Effective Date of this Order, Equifax Inc., its successors and assigns, must pay the civil money penalty by wire transfer to the Bureau or to the Bureau's agent in compliance with the Bureau's wiring instructions.

C. Defendant must treat the penalty paid under this Order as a penalty paid to the government for all purposes. Regardless of how the Bureau ultimately uses those funds, Defendant may not:

1. Claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for the penalty paid under this Order; or

2. Seek or accept, directly or indirectly, reimbursement or indemnification from any source, including but not limited to payment made under any insurance policy, with regard to the penalty paid under this Order.

D. To preserve the deterrent effect of the penalty in any Related Consumer Action, Defendant may not argue that Defendant is entitled to, nor may Defendant benefit by, any offset or reduction of any compensatory monetary remedies imposed in any Related Consumer Action because of the penalty paid in this action. If the court in any Related Consumer Action offsets or otherwise reduces the amount of compensatory monetary remedies imposed against Defendant based on the penalty paid in this action or based on any payment that the Bureau makes from the Civil Penalty Fund, Defendant must, within 30 days after entry of a final order granting such offset or reduction, notify the Bureau, and pay the amount of the offset or reduction to the U.S. Treasury. Such a payment will not be considered an additional civil money penalty and will not change the amount of the civil money penalty imposed in this action.

XIII. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. In the event of any default on Defendant's obligations to make payment under this Order, interest computed under 28 U.S.C. § 1961, as amended, will accrue on any outstanding amounts not paid from the date of default to the date of payment, and will immediately become due and payable.

B. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets, except in the event of a Triggering Event. In that instance, Defendant shall have the right to seek the return of assets deposited into the Fund that have not been disbursed by the Settlement Administrator so that Defendant may provide such assets to the Federal Trade Commission to begin disbursing funds from the Consumer Fund and performing, pursuant to Subsections XI.K-L, all duties and obligations under this Order.

C. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Bureau in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.

D. The facts alleged in the Complaint establish all elements necessary to sustain an action by the Bureau pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.

E. Defendant acknowledges that its Taxpayer Identification Number, which Defendant must submit to the Bureau, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

F. On an annual basis for twenty (20) years following the Effective Date of this Order, Defendant must provide the Enforcement Director in writing with the total number of final judgments, consent orders, or settlements in Related Consumer Actions during the preceding year, as well as the total amount of redress, if any, that Defendant paid or was required to pay to consumers pursuant to those Related Consumer Actions, and describe the consumers or classes of consumers to whom that redress, if any, has been or will be paid.

XIV. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this Order:

A. Defendant, within seven (7) days of entry of this Order, must submit to the Bureau an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. Within 30 days of the Effective Date, Defendant must deliver a copy of this Order to all (1) principals, officers, directors, and LLC managers and members, and (2) all employees, managers, agents, representatives, and service providers having managerial or supervisory responsibilities for conduct related to the subject matter of the Order. For ten (10) years from the Effective Date, Defendant must deliver a copy of this Order to: (1) any

business entity resulting from any change in structure as set forth in Section XV; (2) all future board members and executive officers; and (3) all employees, managers, agents, representatives, and service providers having managerial or supervisory responsibilities for conduct related to the subject matter of the Order before the date on which they assume their responsibilities.

C. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order, ensuring that any electronic signatures conform with the requirements of the E-Sign Act, 15 U.S.C. § 7001 *et seq.*

XV. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that Defendant make timely submissions to the Bureau:

A. Within seven (7) days after the entry of this Order, Defendant must identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Bureau may use to communicate with Defendant.

B. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury, in which Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Bureau may use to communicate with Defendant; (b) identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business identified in (b), including the goods or services offered, the means of advertising, marketing, and sales, and the categories or types of Personal Information collected, transferred, maintained, processed or stored by each business; (d) describe in detail whether and how Defendant is in compliance with each Section of this Order; and (e) provide a copy of, or record proving, each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Bureau.

C. For twenty (20) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

D. Defendant must submit to the Bureau notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against the Defendant within fourteen (14) days of its filing.

E. Any submission to the Bureau required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

F. Unless otherwise directed by a Bureau representative in writing, all submissions to the Bureau pursuant to this Order must be emailed to Enforcement_Compliance@cfpb.gov and sent by overnight courier or first class mail to Enforcement Director, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin "Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02."

XVI. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for twenty (20) years after entry of the Order, and retain each such record for five (5) years. Specifically, Defendant must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reasons for termination;

C. Copies of records of all U.S. consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;

D. Copies of final judgments, consent orders, or settlements in Related Consumer Actions;

E. A copy of each information security assessment required by this Order and any material evaluations of Defendant's physical, technical, or administrative controls to protect the confidentiality, integrity, or availability of Personal Information;

F. A copy of each widely disseminated and unique representation by Defendant that describes the extent to which Defendant maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information;

G. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that are in Defendant's possession and control that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Defendant, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Defendant's compliance with related Sections of this Order, for the compliance period covered by such Assessment; and

H. All records necessary to demonstrate full compliance with each Section of this Order; including all submissions to the Bureau.

XVII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Defendant's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Bureau, Defendant must: submit additional compliance reports or other requested information, related to the requirements of this Order, which must be sworn under penalty of perjury; provide sworn testimony and appear for depositions; and produce documents related to the requirements of this Order and Defendant's compliance with those requirements, for inspection and copying. The Bureau is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Bureau is authorized to communicate directly with Defendant. Defendant must permit representatives of the Bureau to interview any employee or other person affiliated with Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Bureau may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Bureau's lawful use of civil investigative demands under 12. C.F.R. § 1080.6 (2018) or other compulsory process.

XVIII. SEVERABILITY

IT IS FURTHER ORDERED that if any clause, provision, or section of this Order shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Order and this Order shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

XIX. RETENTION OF JURISDICTION

IT IS FUTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this _____ day of _____, 2019.

Judge Thomas W. Thrash, Jr.
United States District Court Chief Judge

LOCAL COUNSEL:

BYUNG J. PAK
United States Attorney

/s/ Akash Desai
AKASH DESAI
Assistant U.S. Attorney
Georgia Bar No. 338124
600 U.S. Courthouse
75 Ted Turner Drive SW
Atlanta, Georgia 30303
Telephone: 404-581-6364
Facsimile: 404-581-6181

FOR PLAINTIFF:

BUREAU OF CONSUMER FINANCIAL PROTECTION

CARA PETERSEN
Acting Enforcement Director

JOHN WELLS
Deputy Enforcement Director

/s/ Jenelle M. Dennis
JENELLE M. DENNIS
D.C. Bar No. 494958
RICHA DASGUPTA
D.C. Bar No. 500509
P. SOLANGE HILFINGER-PARDO
California Bar No. 320055
EMILY MINTZ SACHS
Virginia Bar No. 82437
Bureau of Consumer Financial Protection
1700 G Street, NW
Washington, DC 20552
Telephone: (202) 435-9118 (Dennis)
Facsimile: (202) 425-7722
Email: jenelle.dennis@cfpb.gov

FOR DEFENDANT:

/s/ John J. Kelley III
JOHN J. KELLEY III
Corporate Vice President,
Chief Legal Officer
Equifax Inc.
1550 Peachtree Street, NW
Atlanta, GA 30309

Date: 7/19/19

/s/ Edith Ramirez
EDITH RAMIREZ
HARRIET PEARSON
MICHELLE KISLOFF
TIMOTHY TOBIN
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
Tel: (202) 637-5600
Fax: (202) 637-5910

Date: 7/19/19

EX-10.4 5 d734596dex104.htm EX-10.4

Exhibit 10.4

IN THE CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA

THE STATE OF ALABAMA ex rel., STEVE MARSHALL, ATTORNEY GENERAL	)	
Plaintiff,	)	
v.	)	**Case No. _____**
EQUIFAX, INC.	)	
Defendant.	)	

FINAL JUDGMENT AND CONSENT DECREE

Plaintiff, the State of Alabama, by Steve Marshall, Attorney General of the State of Alabama, has filed a Complaint for a permanent injunction and other relief in this matter pursuant to the Alabama Deceptive Trade Practices Act, Sections 8-19-1 through -15 of the Alabama Code, alleging that Defendant EQUIFAX, INC. ("EQUIFAX"), appearing through its attorney, King & Spalding LLP, has committed violations of the Deceptive Trade Practices Act.

Plaintiff and EQUIFAX have agreed to the Court's entry of this Final Judgment and Consent Decree without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by EQUIFAX regarding any issue of law or fact alleged in the Complaint on file, without EQUIFAX admitting any liability, and with all parties having waived their right to appeal. This Court, having considered the matter and finding good cause appearing, hereby **ORDERS, ADJUDGES, AND DECREES** as follows:

I. PARTIES AND JURISDICTION

1. The Attorney General is charged with enforcement of the Deceptive Trade Practices Act. *See* Ala. Code § 8-19-4.

2. Defendant EQUIFAX, Inc. is the parent of EQUIFAX INFORMATION SERVICES, LLC ("EIS"), a CONSUMER REPORTING AGENCY, with its principal office located at 1550 Peachtree St. NW, Atlanta, Georgia 30309.

3. This Court has jurisdiction over the subject matter of the complaint filed herein and over the parties to this Final Judgment and Consent Decree.

4. Defendant, at all relevant times, has transacted business in the State of Alabama, including, but not limited to, Jefferson County.

5. This Judgment is entered pursuant to and subject to the Deceptive Trade Practices Act, Ala. Code § 8-19-1, *et seq.*

II. DEFINITIONS

6. For the purposes of this Judgment, the following definitions shall apply:

a. “2017 DATA BREACH” shall mean the data breach, first publicly announced by EQUIFAX on September 7, 2017, in which a person or persons gained unauthorized access to portions of the EQUIFAX NETWORK.

b. “2017 BREACH RESPONSE SERVICES AND PRODUCTS” shall mean the following complimentary support services and/or products provided by EQUIFAX, its affiliates, or third parties retained by EQUIFAX or its affiliates, in response to the 2017 DATA BREACH: TrustedID Premier; Equifax Credit Watch Gold with 3-in-1 Monitoring (offered to consumers as a print alternative to TrustedID Premier); the IDNotify product offered for free through Experian; Lock & Alert; and the credit protection services required by Paragraph 42.

c. “AFFECTED CONSUMERS” shall mean all consumers residing in Alabama who had their PERSONAL INFORMATION accessed by any unauthorized individual in connection with the 2017 DATA BREACH.

d. "ATTORNEYS GENERAL" shall mean the Attorneys General of the states and commonwealths of: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii,[1] Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah,[2] Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming, and the District of Columbia.

e. "CLEARLY AND CONSPICUOUSLY" shall mean that such statement, disclosure, or other information, by whatever medium communicated, including all electronic devices, is (a) in readily understandable language and syntax, and (b) in a type size, font, color, appearance, and location sufficiently noticeable for a consumer to read and comprehend it, in a print that contrasts with the background against which it appears.

i. If such statement, disclosure, or other information is necessary as a modification, explanation, or clarification to other information with which it is presented, it must be presented in proximity to the information it modifies in a manner that is readily noticeable and understandable; and

ii. In any communication using an interactive electronic medium, such as the internet or software, the disclosure must be obvious.

---

1 Hawaii is represented by its Office of Consumer Protection. For simplicity purposes, the entire group will be referred to as the "Attorneys General," or individually as "Attorney General." Such designations, however, as they pertain to Hawaii, shall refer to the Executive Director of the State of Hawaii Office of Consumer Protection.

2 Claims pursuant to the Utah Protection of Personal Information Act are brought under the direct enforcement authority of the Attorney General. Utah Code § 13-44-301(1). Claims pursuant to the Utah Consumer Sales Practices Act are brought by the Attorney General as counsel for the Utah Division of Consumer Protection, pursuant to the Division's enforcement authority. Utah Code §§ 13-2-1 and 6.

f. “COMPENSATING CONTROLS” shall mean alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer or his or her designee to be impractical to implement at the present time due to legitimate technical or business constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of security as the original stated requirement; (3) be up-to-date with current industry accepted security protocols; and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable.

g. “CONSUMER REPORTING AGENCY” shall mean any person as defined by 15 U.S.C. § 1681a(p), and any amendments thereto.

h. “CREDIT FILE” shall mean a file as defined in 15 U.S.C. § 1681a(g), and any amendments thereto.

i. “CREDIT REPORT” shall mean a consumer report as defined in 15 U.S.C. § 1681a(d), and any amendments thereto.

j. “EFFECTIVE DATE” shall be August 22, 2019 except as otherwise noted in the Judgment.

k. “ENCRYPT,” “ENCRYPTED,” or “ENCRYPTION” shall mean rendering data—at rest or in transit—unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security commensurate with the sensitivity of the data at issue.

l. “EQUIFAX” shall mean Equifax Inc., its affiliates, directors, officers, subsidiaries and divisions, successors and assigns doing business in the United States.

m. “EQUIFAX NETWORK” shall mean all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of using and sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by EQUIFAX; and (3) collect, process, store, or have access to PERSONAL INFORMATION of consumers who reside in the United States. For purposes of this Judgment, EQUIFAX NETWORK shall not include networking equipment, databases or data stores, applications, servers, or endpoints outside of the United States, which are not used to collect, process, or store PERSONAL INFORMATION, and where access to PERSONAL INFORMATION is restricted using a risk-based control. For purposes of this definition, a risk-based control shall, at a minimum, include: (i) web-application-, network-, or host-based firewalls, or ENCRYPTION of the PERSONAL INFORMATION; and (ii) preadmission identification and/or access management controls, including, for example, multi-factor authentication.

n. “FCRA” shall mean the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, and any amendments thereto.

o. “FEE-BASED PRODUCTS OR SERVICES” shall mean any product or service that EQUIFAX sells or charges any amount of money for United States consumers to use or obtain.

p. “FURNISHER” or “FURNISHERS” shall mean a person or entity that meets the definition of furnisher set forth in 16 C.F.R. § 660.2(c), and any amendments thereto.

q. “GOVERNANCE PROCESS” shall mean any written policy, standard, procedure, or process (or any combination thereof) designed to achieve a control objective with respect to the EQUIFAX NETWORK.

r. “MULTI-DISTRICT LITIGATION” shall mean those actions filed against Equifax Inc. and/or its subsidiaries asserting claims related to the 2017 DATA BREACH by or on behalf of one or more consumers that have been or will be transferred to the federal proceedings styled In re Equifax Inc. Customer Data Security Breach Litigation, MDL 1:17-md-2800 (N.D. Ga.) (Consumer Actions).

s. "MULTISTATE LEADERSHIP COMMITTEE" shall mean California, Connecticut, District of Columbia, Florida, Georgia, Illinois, Maryland, New Jersey, New York, Ohio, and Pennsylvania.

t. "NON-FCRA INFORMATION" shall mean any information that is collected, stored, or maintained by EQUIFAX and either:

i. Does not bear on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, or

ii. Is not used or expected to be used or collected in whole or in part for any purpose authorized under 15 U.S.C. § 1681b, and any amendments thereto.

u. "PERSONAL INFORMATION" shall mean information regarding an individual residing in Alabama that falls within one of the following categories:

i. A consumer's first name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number; (c) state- or federally-issued identification card number; or (d) financial account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial account;

ii. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical characteristics or digital representation thereof;

iii. A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or

iv. Any category of personal information found in the definition of "SENSITIVE PERSONALLY IDENTIFYING INFORMATION" as set forth in the Alabama Data Breach Notification Act of 2018, Section 8-38-2(6) through -12 of the Code of Alabama.

v. "PROTECTED INDIVIDUAL" shall mean an individual who meets the definition of protected consumer set forth in 15 U.S.C. § 1681c-1(j)(1)(B), and any amendments thereto.

w. "REINVESTIGATION" or "REINVESTIGATE" shall mean the process set forth in 15 U.S.C. § 1681i, and any amendments thereto.

x. "SECURITY EVENT" shall mean any compromise, or threat that gives rise to a reasonable likelihood of compromise, by unauthorized access or inadvertent disclosure impacting the confidentiality, integrity, or availability of PERSONAL INFORMATION of at least 500 United States consumers held or stored within the EQUIFAX NETWORK, including but not limited to a data breach. For purposes of this definition, "availability" shall not include an intentional limitation on the availability of PERSONAL INFORMATION, such as for purposes of performing maintenance on the EQUIFAX NETWORK.

III. INJUNCTIVE RELIEF

7. The duties, responsibilities, burdens, and obligations undertaken in connection with this Judgment shall apply to EQUIFAX, and its directors, officers, and employees.

8. The injunctive terms contained in this Final Judgment and Consent Decree are being entered pursuant to Section 8-19-8 of the Code of Alabama.

COMPLIANCE WITH LAW

9. EQUIFAX shall comply with the Deceptive Trade Practices Act and the Alabama Data Breach Notification Act of 2018 in connection with its collection, maintenance, and safeguarding of PERSONAL INFORMATION of consumers in Alabama.

10. EQUIFAX shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which EQUIFAX maintains and/or protects the privacy, security, confidentiality, or integrity of any PERSONAL INFORMATION collected from or about consumers.

11. EQUIFAX shall not offer, provide, or sell any good or service in violation of 15 U.S.C. § 1681c-1(i), and any amendments thereto.

12. EQUIFAX shall comply with the Alabama Data Breach Notification Act of 2018, Ala. Code § 8-38-1, *et seq*.

INFORMATION SECURITY PROGRAM

13. Within ninety (90) days after the EFFECTIVE DATE and for a period of seven (7) years, EQUIFAX shall implement, maintain, regularly review and revise, and comply with a comprehensive information security program ("Information Security Program") the purpose of which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of PERSONAL INFORMATION on the EQUIFAX NETWORK. EQUIFAX's Information Security Program shall be documented in the GOVERNANCE PROCESSES and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of EQUIFAX's operations;

b. The nature and scope of EQUIFAX's activities; and

c. The sensitivity of the PERSONAL INFORMATION on the EQUIFAX NETWORK.

The Information Security Program required by this Judgment shall include the requirements of Paragraphs 14 through 40 in this Judgment.

14. The principles of zero-trust should be considered and, where reasonably feasible, utilized in the design of EQUIFAX's Information Security Program.

15. EQUIFAX may satisfy the implementation and maintenance of the Information Security Program and the safeguards required by this Judgment through review, maintenance, and, if necessary, updating, of an existing information security program or existing safeguards, provided that such existing information security program and existing safeguards meet the requirements set forth in this Judgment.

16. EQUIFAX shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (for ease, hereinafter referred to as the "Chief Information Security Officer"). The Chief Information Security Officer shall have the education, qualifications, and experience appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. This Chief Information Security Officer shall report annually to the EQUIFAX Board of Directors on the adequacy of EQUIFAX's Information Security Program. The Chief Information Security Officer shall also, at any meeting of the Board of Directors concerning the security posture or security risks faced by EQUIFAX and at each quarterly meeting of the Technology Committee of the Board of Directors, provide reports to EQUIFAX's Board of Directors, and shall inform, advise, and update the Board of Directors or Technology Committee regarding

EQUIFAX's security posture and the security risks faced by EQUIFAX. The Chief Information Security Officer shall report to the Chief Executive Officer, as well as a member of EQUIFAX's Board of Directors, in the event that the Chief Executive Officer is not a member of the Board of Directors, (i) any unauthorized intrusion to the EQUIFAX NETWORK within forty-eight (48) hours of discovery that it is a SECURITY EVENT and (ii) any "THIRD-PARTY REPORTED EVENT" as defined in Paragraph 23 within forty-eight (48) hours of receipt of the report from the third-party vendor. The quarterly reports to the Technology Committee shall also include all SECURITY EVENTS or THIRD-PARTY REPORTED EVENTS that were reported to the Chief Executive Officer after the previous regular report.

17. EQUIFAX shall employ for each of its United States business units an officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program for that business unit (for ease, hereinafter referred to as a "Business Information Security Officer"). Each Business Information Security Officer shall have the education, qualifications, and experience appropriate to the level, size, and complexity of the Business Information Security Officer's role in implementing, maintaining and monitoring the Information Security Program. Each Business Information Security Officer shall be responsible for regularly informing, advising, and updating the Chief Information Security Officer or his/her designee regarding the security posture of the business unit for which he/she is responsible, the security risks faced by the relevant business units, and the implications of any decision the Business Information Security Officer makes that may materially impact the security posture of the business unit.

18. EQUIFAX shall ensure that the Chief Information Security Officer, Business Information Security Officers, and Information Security Program receive the resources and support reasonably necessary to ensure that the Information Security Program functions as required by this Judgment.

19. Employees who are responsible for implementing, maintaining, or monitoring the Information Security Program, including but not limited to the Chief Information Security Officer and Business Information Security Officers, must have sufficient knowledge of the requirements of this Judgment and receive specialized training on safeguarding and protecting consumer PERSONAL INFORMATION to help effectuate EQUIFAX's compliance with the terms of this Judgment. EQUIFAX shall provide the training required under this paragraph to all employees within sixty (60) days of the EFFECTIVE DATE of this Judgment or prior to an employee starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program. On an annual basis, or more frequently if appropriate, EQUIFAX shall provide training on safeguarding and protecting PERSONAL INFORMATION to its employees who handle PERSONAL INFORMATION, and its employees responsible for implementing, maintaining, or monitoring the Information Security Program.

20. EQUIFAX's Information Security Program shall be designed and implemented to ensure the appropriate identification, investigation of, and response to SECURITY EVENTS.

21. EQUIFAX shall implement and maintain a written incident response plan to prepare for and respond to SECURITY EVENTS. EQUIFAX shall revise and update this response plan, as necessary, to adapt to any changes to the EQUIFAX NETWORK. Such a plan shall, at a minimum, identify and describe the following phases:

I. Preparation;

II. Detection and Analysis;

III. Containment;

IV. Notification and Coordination with Law Enforcement;

V. Eradication;

VI. Recovery;

VI. Consumer Response (including consideration of appropriate staffing levels, training, and written materials), and Consumer and Regulator Notification and Remediation; and

VII. Post-Incident Analysis.

22. EQUIFAX shall conduct, at a minimum, biannual incident response plan exercises ("table-top exercises") to test and assess its preparedness to respond to a SECURITY EVENT. These exercises shall include the following, as appropriate:

a. Planning for sufficient staffing levels to handle a high volume of potential consumer traffic and provide consumers access to live agents in a reasonable amount of time;

b. Planning employee training to provide relevant, useful, and accurate information to consumers, including how to place fraud alerts or security freezes;

c. Preparing written materials to provide to consumers that CLEARLY AND CONSPICUOUSLY disclose relevant information;

d. Planning for any necessary online resources to be compliant with the Americans with Disabilities Act (ADA);

e. Planning for oral and written consumer communications in multiple languages depending on the nature of the table-top exercise; and

f. Considering the translation of state-required data breach notifications to consumers into multiple languages including Spanish, Chinese, Tagalog, Vietnamese, Arabic, French, and Korean depending on the nature of the table-top exercise.

23. EQUIFAX shall oversee its third-party vendors who have access to the EQUIFAX NETWORK or who hold or store PERSONAL INFORMATION on EQUIFAX's behalf by maintaining and periodically reviewing and revising, as needed, a GOVERNANCE PROCESS for assessing vendor compliance in accordance with EQUIFAX'S Information Security Program including whether the vendor's security safeguards are appropriate for that business. That GOVERNANCE PROCESS shall require vendors by contract to implement and maintain such safeguards and to notify EQUIFAX within seventy-two (72) hours of discovering a SECURITY EVENT (a "THIRD-PARTY REPORTED EVENT").

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

24. EQUIFAX shall maintain and comply with a GOVERNANCE PROCESS establishing that PERSONAL INFORMATION will be collected, processed, or stored to the minimum extent necessary to accomplish the intended legitimate business purpose(s) in using such information.

25. EQUIFAX shall maintain, regularly review, revise, and comply with a GOVERNANCE PROCESS requiring EQUIFAX to either ENCRYPT PERSONAL INFORMATION or otherwise implement COMPENSATING CONTROLS to protect PERSONAL INFORMATION from unauthorized access, whether the information is transmitted electronically from the EQUIFAX NETWORK or is stored in the EQUIFAX NETWORK.

26. EQUIFAX shall make reasonable efforts to reduce its use and storage of consumer Social Security numbers. It shall:

a. Actively seek to and, where possible, participate in an external organization or working group focused on the development and implementation of alternative means of identity authentication with a goal of identifying options for minimizing its use of Social Security numbers for identity authentication purposes, to the extent that any such group exists;

b. Conduct an internal study of the primary instances in which Social Security numbers are collected, maintained, or used on the EQUIFAX NETWORK, including for consumer authentication purposes, and evaluate potential alternatives to such collection, maintenance, or use. In evaluating such alternatives, EQUIFAX may consider, among other things, the impact on privacy, security, reducing identity theft and fraud, and ease of incorporation into EQUIFAX's business processes. Upon the conclusion of this study, or within one year of the EFFECTIVE DATE, whichever is sooner, the study shall be provided to the Chief Executive Officer, who shall establish a working group to implement identified alternatives, where feasible. EQUIFAX shall also provide a copy of the study to the California Attorney General's Office.

i. The California Attorney General's Office may provide a copy of the study received from EQUIFAX to the Alabama Attorney General upon request.

ii. The study and all information contained therein, to the extent permitted by the laws of the State of Alabama: shall be treated by the Alabama Attorney General's Office as confidential; shall not be shared or disclosed except as described in subsection (i); and shall be treated by the Alabama Attorney General's Office as exempt from disclosure under the relevant public records laws of the State of Alabama. In the event that the Alabama Attorney General's Office receives any request from the public for the study or other confidential documents under this Judgment and believes that such information is subject to disclosure under the relevant public records laws, the Alabama Attorney General's Office agrees to provide EQUIFAX with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that EQUIFAX may take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with the notice requirements contained in Paragraph 81. Nothing contained in this subparagraph shall alter or limit the obligations of the Alabama Attorney General that may be imposed by the relevant public records laws of the State of Alabama, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Alabama Attorney General except with respect to the obligation to notify EQUIFAX of any potential disclosure.

c. Maintain authentication protocols that do not allow consumers to access PERSONAL INFORMATION from EQUIFAX in connection with direct-to-consumer products and services, such as credit monitoring and CREDIT REPORTS, using only a name in combination with a Social Security number; and

d. Implement a GOVERNANCE PROCESS that contractually requires EQUIFAX reseller customers who receive consumer PERSONAL INFORMATION from EQUIFAX to maintain authentication protocols that do not allow consumers to access PERSONAL INFORMATION from EQUIFAX in connection with direct-to-consumer products and services, such as credit monitoring and CREDIT REPORTS using only a name in combination with a Social Security number.

27. EQUIFAX shall ENCRYPT Social Security numbers when they are stored in the EQUIFAX NETWORK or transmitted electronically from the EQUIFAX NETWORK, or otherwise implement COMPENSATING CONTROLS to protect Social Security numbers from unauthorized access.

28. EQUIFAX shall maintain, regularly review and revise as necessary, and comply with a GOVERNANCE PROCESS that provides for the secure disposal, using a method that is consistent with Section 8-38-10 of the Code of Alabama, on a periodic basis, of PERSONAL INFORMATION that is no longer necessary for the legitimate business purpose for which the PERSONAL INFORMATION was collected, processed, or stored, except where such information is otherwise required to be maintained by law.

SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

29. **Managing Critical Assets:** EQUIFAX shall rate all software and hardware within the EQUIFAX NETWORK based on criticality, factoring in whether such assets are used to collect, process, or store PERSONAL INFORMATION.

30. **Segmentation:**

a. EQUIFAX shall maintain, regularly review and revise as necessary, and comply with its segmentation protocols and related policies that are reasonably designed to properly segment the EQUIFAX NETWORK, which shall, at a minimum, ensure that systems communicate with each other in a secure manner and only to the extent necessary to perform their business and/or operational functions, and that databases are segmented except from systems with which they are required to interact.

b. EQUIFAX shall regularly evaluate, and, as appropriate, restrict and/or disable any unnecessary ports on the EQUIFAX NETWORK.

c. EQUIFAX shall logically separate its production and non-production environments in the EQUIFAX NETWORK, including the use of appropriate technological safeguards to protect PERSONAL INFORMATION within non-production environments.

31. **Penetration Testing/Risk Assessment:**

a. EQUIFAX shall maintain and regularly review and revise as necessary a risk-assessment program designed to continually identify and assess risks to the EQUIFAX NETWORK. In cases where EQUIFAX deems a risk to be acceptable, EQUIFAX shall generate and retain a report demonstrating how such risk is to be managed in consideration of cost or difficulty in implementing effective countermeasures. All reports shall be maintained by the Chief Information Security Officer or his or her designee and be available for inspection by the Third-Party Assessor described in Paragraph 61 of this Judgment.

b. EQUIFAX shall implement and maintain a risk-based penetration-testing program reasonably designed to identify, assess, and remediate security vulnerabilities within the EQUIFAX NETWORK. This program shall include at least one annual penetration test of all externally-facing applications within the EQUIFAX NETWORK and at least one weekly vulnerability scan of all systems within the EQUIFAX NETWORK.

c. EQUIFAX shall rate and rank the criticality of all vulnerabilities identified as a result of any vulnerability scanning or penetration testing that it performs on the EQUIFAX NETWORK in alignment with an established industry-standard framework (e.g., NVD, CVSS, or equivalent standard). For each vulnerability that is ranked as most critical, EQUIFAX shall commence remediation planning within twenty-four (24) hours after the vulnerability has been rated as critical and shall apply the remediation within one (1) week after the vulnerability has received a critical rating. If the remediation cannot be applied within one (1) week after the vulnerability has received a critical rating, EQUIFAX shall identify existing or implement new COMPENSATING CONTROLS designed to protect PERSONAL INFORMATION as soon as practicable but no later than one (1) week after the vulnerability received a critical rating.

32. **Access Control and Account Management:**

a. EQUIFAX shall implement and maintain appropriate controls to manage access to, and use of, all EQUIFAX NETWORK accounts with access to PERSONAL INFORMATION, including, without limitation, individual accounts, administrator accounts, service accounts, and vendor accounts. To the extent that EQUIFAX maintains accounts requiring passwords:

i. Such controls shall include strong passwords, password confidentiality policies, password-rotation policies, and two-factor authentication or any other equal or greater authentication protocol, where technically feasible. For purposes of this paragraph, any administrative-level passwords shall be ENCRYPTED or secured using a password vault, privilege access monitoring, or an equal or greater security tool that is generally accepted by the security industry.

ii. EQUIFAX shall implement and maintain appropriate policies for the secure storage of EQUIFAX NETWORK account passwords based on industry best practices; for example, hashing passwords stored online using an appropriate hashing algorithm that is not vulnerable to a collision attack together with an appropriate salting policy, or other equivalent or stronger protections.

b. EQUIFAX shall implement and maintain adequate access controls, processes, and procedures, the purpose of which shall be to grant access to the EQUIFAX NETWORK only after the user has been properly identified, authenticated, reviewed, and approved.

c. EQUIFAX shall as soon as practicable, and within forty-eight (48) hours, terminate access privileges for all persons whose access to the EQUIFAX NETWORK is no longer required or appropriate.

d. EQUIFAX shall limit access to PERSONAL INFORMATION by persons accessing the EQUIFAX NETWORK on a least-privileged basis.

e. EQUIFAX shall regularly inventory the users who have access to the EQUIFAX NETWORK in order to review and determine whether or not such access remains necessary or appropriate. EQUIFAX shall regularly compare termination lists to user accounts to ensure access privileges have been appropriately terminated. At a minimum, such review shall be performed on a quarterly basis.

f. EQUIFAX shall implement and maintain adequate administration processes and procedures to store and monitor the account credentials and access privileges of employees who have privileges to design, maintain, operate, and update the EQUIFAX NETWORK.

g. EQUIFAX shall implement and maintain controls to identify and prevent unauthorized devices from accessing the EQUIFAX NETWORK such as a network access controller or similar or more advanced technology.

33. **File Integrity Monitoring:** EQUIFAX shall maintain controls designed to provide near real-time notification of unauthorized modifications to the EQUIFAX NETWORK. The notification shall include information available about the modification including, where available, the date of the modification, the source of the modification, the type of modification, and the method used to make the modification.

34. **Unauthorized Applications:** EQUIFAX shall maintain controls designed to identify and protect against the execution or installation of unauthorized applications on the EQUIFAX NETWORK.

35. **Logging and Monitoring:**

a. EQUIFAX shall implement controls the purposes of which shall be to monitor and log material security and operational activities on the EQUIFAX NETWORK, to report anomalous activity through the use of appropriate platforms, and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance.

b. All SECURITY EVENTS shall immediately be reported to the Chief Information Security Officer and appropriate Business Information Security Officer, and in no event more than eight (8) hours from the identification of the SECURITY EVENT. Any vulnerability that is associated with a SECURITY EVENT shall be remediated within twenty-four (24) hours of the identification of the vulnerability. If that vulnerability cannot be remediated within twenty-four (24) hours of its identification, then EQUIFAX shall implement COMPENSATING CONTROLS or decommission the system within twenty-four (24) hours of the identification of the vulnerability.

c. EQUIFAX shall monitor on a daily basis, and shall test on at least a monthly basis, any tool used pursuant to this paragraph, to properly configure, regularly update, and maintain the tool, to ensure that the EQUIFAX NETWORK is adequately monitored.

36. **Change Control:** EQUIFAX shall maintain, regularly review and revise as necessary, and comply with a GOVERNANCE PROCESS established to manage and document changes to the EQUIFAX NETWORK. At a minimum:

a. EQUIFAX shall define the roles and responsibilities for those involved in the change control process, including a board responsible for reviewing changes (for ease, hereinafter referred to as the "Change Advisory Board"). The Change Advisory Board shall include stakeholders from the appropriate business and informational technology units. The Change Advisory Board's responsibilities shall include: managing overall change control policies and procedures; providing guidance regarding the overall change control policies and procedures; conducting an annual audit of change requests to ensure that changes to the EQUIFAX NETWORK are properly analyzed and prioritized; and reviewing, approving, evaluating, and scheduling requests for changes to the EQUIFAX NETWORK.

b. The change control policies and procedures shall address the process to: request a change to the EQUIFAX NETWORK; determine the priority of the change; determine the change's impact on the EQUIFAX NETWORK, the security of PERSONAL INFORMATION, and EQUIFAX's ongoing business operations; obtain the appropriate approvals from required personnel (e.g., change requester, business unit, Business Information Security Officer, Change Advisory Board); develop, test, and implement the change; and review and test the impact of

the change on the EQUIFAX NETWORK and the security of PERSONAL INFORMATION after the change has been made. The change control policies and procedures required by this paragraph shall require that any changes to the EQUIFAX NETWORK be evaluated regarding potential risks, and that all changes receive appropriate additional or heightened (i) analysis, (ii) approvals from required personnel, and (iii) testing.

c. Any action with respect to any changes to the EQUIFAX NETWORK (requesting, analyzing, approving, developing, implementing, and reviewing) shall be documented and retained, with the documentation appropriately secured and stored in repositories that are scoped to an application, business unit, and/or geography and are accessible to appropriate security personnel.

37. **Asset Inventory:** EQUIFAX shall utilize manual processes and, where practicable, automated tool(s) to regularly inventory and classify, and issue reports on, all assets that comprise the EQUIFAX NETWORK, including but not limited to all software, applications, network components, databases, data stores, tools, technology, and systems. The asset inventory as well as applicable configuration and change management systems shall, at a minimum, collectively identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the EQUIFAX NETWORK; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores PERSONAL INFORMATION; and (g) each security update and security patch applied or installed during the preceding period.

38. **Digital Certificates:** EQUIFAX shall implement and maintain a digital certificate management tool or service the purpose of which shall be to inventory digital certificates that expire longer than a week after their creation and that are used to authenticate servers and systems in the EQUIFAX NETWORK. The system or tool required by this paragraph shall manage the life cycle of all such digital certificates, including whether to issue, cancel, renew, reissue, or revoke a digital certificate. The system or tool required by this paragraph shall track the expiration date of any such digital certificate and provide notification of such expiration to the custodian of the certificate key thirty days (30) prior to expiration, ten days (10) prior to expiration, and on the date the digital certificate expires. Digital certificate for purposes of this paragraph shall include a security token, biometric identifier, or a cryptographic key used to protect externally-facing systems and applications.

39. **Threat Management:** EQUIFAX shall establish a threat management program which shall include the use of automated tools to continuously monitor the EQUIFAX NETWORK for active threats. EQUIFAX shall monitor on a daily basis, and shall test on at least a monthly basis, any tool used pursuant to this paragraph, to assess whether the monitoring tool is regularly configured, tested, and updated.

40. **Updates/Patch Management:** EQUIFAX shall maintain, keep updated, and support the software on the EQUIFAX NETWORK, taking into consideration the impact a software update will have on data security in the context of the EQUIFAX NETWORK and its ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. At a minimum, EQUIFAX shall also do the following:

a. For any software that will no longer be supported by its manufacturer or a third party, EQUIFAX shall commence the evaluation and planning to replace the software or to maintain the software with appropriate COMPENSATING CONTROLS at least two (2) years prior to the date on which the manufacturer's or third party's support will cease, or from the date the manufacturer or third party announces that it is no longer supporting the software if such period is less than two (2) years. If EQUIFAX is unable to commence the evaluation and planning in the timeframe required by this subparagraph, it shall prepare and maintain a written exception that shall include:

i. A description of why the exception is appropriate, e.g., what business need or circumstance supports the exception;

ii. An assessment of the potential risk posed by the exception; and

iii. A description of the schedule that will be used to evaluate and plan for the replacement of the software or addition of any COMPENSATING CONTROLS.

b. EQUIFAX shall maintain reasonable controls to address the potential impact security updates and security patches may have on the EQUIFAX NETWORK and shall:

i. Maintain a patch management solution(s) to manage software patches that includes the use of automated, standardized patch management distribution tool(s), whenever technically feasible, to: maintain a database of patches; deploy patches to endpoints; verify patch installation; and retain patch history. The patch management program must also have a dashboard or otherwise report on the success, failure, or other status of any security update or security patch; and

ii. Maintain a tool that includes an automated Common Vulnerabilities and Exposures (CVE) feed. The CVE tool required by this subparagraph shall provide EQUIFAX regular updates throughout each day regarding known CVEs for vendor-purchased software applications in use within the EQUIFAX NETWORK. EQUIFAX may satisfy its obligations under this subparagraph by using an industry-standard vulnerability scanning tool. The CVE tool required by this subparagraph shall also:

(a) Identify, confirm, and enhance discovery of the parts of the EQUIFAX NETWORK that may be subject to CVE events and/or incidents;

(b) Scan the EQUIFAX NETWORK for CVEs; and

(c) Scan the EQUIFAX NETWORK to determine whether scheduled security updates and patches have been successfully installed, including whether any security updates or patches rated as critical have been installed consistent with the requirement of this Judgment.

c. EQUIFAX shall appoint an individual ("Patch Supervisor") who shall report up to the Chief Technology Officer and shall be responsible for overseeing a team ("Patch Management Group") of other individuals responsible for regularly reviewing and maintaining the requirements set forth in this paragraph. The Patch Supervisor and the members of the Patch Management Group shall include persons with appropriate experience and qualifications.

d. The Patch Management Group shall be responsible for:

i. Monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from the tools installed pursuant to subparagraph (b) and ensuring the appropriate and timely application of all security updates and/or security patches;

ii. Monitoring compliance with policies and procedures regarding ownership, supervision, evaluation, and coordination of the maintenance, management, and application of all security patches and software and application security updates by appropriate information technology (IT) application and system owners;

iii. Supervising, evaluating, and coordinating any system patch management tool(s) such as those identified in subparagraph (b); and

iv. A training requirement for individuals responsible for implementing and maintaining EQUIFAX's patch management policies.

e. EQUIFAX shall use the inventory created pursuant to Paragraph 37 in its regular operations to assist in identifying assets within the EQUIFAX NETWORK for purposes of applying security updates or security patches that have been released.

f. EQUIFAX shall employ processes and procedures to ensure the timely scheduling and installation of any security update and security patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the EQUIFAX NETWORK, the impact on EQUIFAX's ongoing business and network operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by the United States Computer Emergency Readiness Team

(US-CERT). Such patch management policies shall require EQUIFAX to rate as critical, high, medium, or low all patches and/or updates, rating as "critical" all patches or updates intended to prevent any vulnerability that threatens the safeguarding or security of any PERSONAL INFORMATION maintained on the EQUIFAX NETWORK. If EQUIFAX does not accept or increase the risk ratings disseminated by either a software or application vendor or US-CERT for externally-facing applications on the EQUIFAX NETWORK, EQUIFAX shall identify for any update or patch for which it is attaching the lower risk rating, the assets to which it applies, and create a written explanation that shall include:

i. A description of why the lowered risk rating is appropriate, e.g., what business need or circumstance exists that supports the rating;

ii. A description of the alternatives that were considered, and why they were not appropriate;

iii. An assessment of the potential risks posed by the revised risk rating;

iv. The anticipated length of time for the rating, if the revised risk rating is temporary; and

v. To the extent applicable, a plan for managing or mitigating those risks identified in subparagraph iii (e.g. COMPENSATING CONTROLS, alternative approaches, methods). The written explanation required by this subparagraph shall be prepared within twenty-four (24) hours of its determination to apply a lower rating, and upon revising the rating, the update or patch shall be treated under EQUIFAX's applicable patch management policies, standards, or procedures in accordance with its revised rating.

g. EQUIFAX shall, within twenty-four (24) hours, if feasible, but not later than forty-eight (48) hours of rating any security update or patch as critical, either apply the update or patch to the EQUIFAX NETWORK or take the identified application offline until the update or patch has been successfully applied. If EQUIFAX is not able to, within forty-eight (48) hours of rating any security update or patch as critical, either apply the update or patch to the EQUIFAX NETWORK or take the identified application offline, then EQUIFAX shall apply COMPENSATING CONTROLS as appropriate.

h. In connection with the scheduling and installation of any critical patch and/or update, EQUIFAX shall verify that the patch and/or update was applied and installed successfully throughout the EQUIFAX NETWORK. For each security update or security patch rated as critical, EQUIFAX shall maintain records identifying: (1) each critical patch or update that has been applied; (2) the date(s) each patch or update was applied; (3) the assets to which each patch or update was applied; and (4) whether each patch or update was applied and installed successfully (the "Critical Patch Management Records"). The Critical Patch Management Records shall be reviewed on a weekly basis by the Patch Management Group.

i. On at least a biannual basis, EQUIFAX shall perform an internal assessment of its management and implementation of security updates and patches for the EQUIFAX NETWORK. This assessment shall identify (i) all known vulnerabilities to the EQUIFAX NETWORK and (ii) the updates or patches applied to address each vulnerability. The assessment will be formally identified, documented, and reviewed by the Patch Management Group.

41. **Information Security Program Implementation:** EQUIFAX represents that it has worked and will continue to work in good faith to comply with the requirements of the Information Security Program set forth in this Judgment. As to Paragraphs 24, 25, 26(c), 26(d), 27, 34, 37, and 59, only, the Alabama Attorney General's Office agrees that it shall not commence any action, the purpose of which would be to establish a violation of this order or a finding of contempt until on or after December 31, 2019, subject also to the requirements of Paragraph 82, and that it shall not commence any action, the purpose of which would be to establish a violation of Paragraph 30 or a finding of contempt with respect to that paragraph, until on or after December 31, 2020, subject also to the requirements of Paragraph 82.

CONSUMER-RELATED RELIEF

42. **Extended Credit Monitoring Services:** EQUIFAX shall offer AFFECTED CONSUMERS the opportunity to enroll in credit monitoring services to be provided at no cost for an aggregate of ten (10) years, which may be satisfied either through a court-approved settlement in the MULTI-DISTRICT LITIGATION or pursuant to the Federal Trade Commission (FTC) Stipulated Order For Permanent Injunction and Monetary Judgment and the Consumer Financial Protection Bureau (CFPB) Stipulated Order For Permanent Injunction and Monetary Judgment. These credit monitoring services shall consist of the Three-Bureau Credit Monitoring Services set forth in Paragraph 43 and One-Bureau Credit Monitoring Services set forth in Paragraph 44.

43. **Three-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS who file valid claims shall be eligible for at least four (4) years of a free Three-Bureau Credit Monitoring Service. These four (4) years shall be provided in addition to any free credit monitoring services EQUIFAX is currently providing or has previously offered as a result of the 2017 DATA BREACH. The Three-Bureau Credit Monitoring Services may be provided and maintained by an independent third party. The Three-Bureau Credit Monitoring Services shall include:

a. Daily consumer CREDIT REPORT monitoring from each of the three nationwide CONSUMER REPORTING AGENCIES (EIS, Experian, TransUnion) showing key changes to one or more of an AFFECTED CONSUMER's CREDIT REPORTS, including automated alerts when the following occur: new accounts are opened; inquiries or requests for an AFFECTED CONSUMER's CREDIT REPORT for the purpose of obtaining credit; changes to an AFFECTED CONSUMER's address; and negative information, including delinquencies or bankruptcies.

b. On-demand online access to a free copy of an AFFECTED CONSUMER'S Experian CREDIT REPORT, updated on a monthly basis;

c. Automated alerts, using public or proprietary data sources, when data elements submitted by an AFFECTED CONSUMER for monitoring, such as Social Security number, email address, or credit card numbers, appear on suspicious websites, including websites on the "dark web"; and

d. One Million Dollars ($1,000,000) in identity theft insurance to cover costs related to incidents of identity theft or identity fraud, with coverage prior to the AFFECTED CONSUMER's enrollment in the Three-Bureau Credit Monitoring Service, provided the costs result from a stolen identity event first discovered during the policy period and subject to the terms of the insurance policy.

44. **One-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS who file valid claims and enroll in Three-Bureau Credit Monitoring Services shall be eligible for single-bureau credit monitoring services ("One-Bureau Credit Monitoring Services"). EQUIFAX shall provide One-Bureau Credit Monitoring Services upon expiration of the Three-Bureau Credit Monitoring Services to AFFECTED CONSUMERS who enroll in the Three-Bureau Credit Monitoring Services. EQUIFAX shall provide One-Bureau Credit Monitoring Services for the period of time necessary for the aggregate number of years of credit monitoring provided under Paragraphs 43 and 44 to equal ten (10) years. The cost of the One-Bureau Credit Monitoring Services shall not be paid from the Consumer Restitution Fund described in Section V of this Judgment. One-Bureau Credit Monitoring Services will include the following:

a. Daily CREDIT REPORT monitoring from EQUIFAX showing key changes to an AFFECTED CONSUMER's EIS CREDIT REPORT including automated alerts when the following occur: new accounts are opened; inquiries or requests for an AFFECTED CONSUMER's CREDIT REPORT for the purpose of obtaining credit; changes to an AFFECTED CONSUMER's address; and negative information, such as delinquencies or bankruptcies.

b. On-demand online access to a free copy of an AFFECTED CONSUMER's EIS CREDIT REPORT, updated on a monthly basis; and

c. Automated alerts using certain available public and proprietary data sources when data elements submitted by an AFFECTED CONSUMER for monitoring, such as Social Security numbers, email addresses, or credit card numbers, appear on suspicious websites, including websites on the "dark web."

45. For any AFFECTED CONSUMERS who were under the age of 18 on May 13, 2017, EQUIFAX shall offer these consumers who make valid claims the opportunity to enroll in credit monitoring to achieve an aggregate of eighteen (18) years of continuous credit monitoring at no cost, which may be satisfied either through a court-approved settlement in the MULTI-DISTRICT LITIGATION or pursuant to the FTC Stipulated Order For Permanent Injunction and Monetary Judgment. These services shall include:

a. At least four (4) years of Three-Bureau Credit Monitoring Services, except that during the period when an AFFECTED CONSUMER is under the age of 18, the services provided will be child monitoring services where the parent or guardian can enroll the AFFECTED CONSUMER under the age of 18 to receive the following services: alerts when data elements submitted for monitoring appear on suspicious websites, such as websites on the "dark web;" and alerts when the Social Security number of an AFFECTED CONSUMER under the age of 18 is associated with new names or addresses or the creation of a CREDIT REPORT at one or more of the three nationwide CREDIT REPORTING AGENCIES;

b. Followed by no more than fourteen (14) years of One-Bureau Credit Monitoring Services, except that during the period when an AFFECTED CONSUMER is under the age of 18, EQUIFAX will provide child monitoring services where the parent or guardian can enroll the AFFECTED CONSUMER under the age of 18 in these services and must validate their status as guardian. These child monitoring services include: alerts when data elements such as a Social Security number submitted for monitoring appear on suspicious websites, including websites on the "dark web;" for minors who do not have an EIS CREDIT REPORT, an EIS CREDIT REPORT is created, locked, and then monitored, and for minors with an EIS CREDIT REPORT, their EIS CREDIT REPORT is locked and then monitored.

46. EIS shall offer all United States consumers two free copies of their EIS CREDIT REPORT every 12 months, for at least five (5) years from the implementation of this paragraph. EQUIFAX shall implement this paragraph by December 31, 2019.

47. Consistent with, and as required by federal law, EIS shall not collect any fees for creating an EIS CREDIT FILE in connection with a request from a PROTECTED INDIVIDUAL to place a security freeze on his/her EIS CREDIT FILE. Additionally, EIS shall not collect any fees for placing, temporarily lifting, or removing a security freeze on an EIS CREDIT FILE.

48. EQUIFAX shall continue to refrain from charging consumers any fees for any 2017 BREACH RESPONSE SERVICES AND PRODUCTS.

49. EQUIFAX shall not request or collect payment information (such as payment card information or financial account information) from consumers during their enrollment process for any 2017 BREACH RESPONSE SERVICES AND PRODUCTS regardless of whether such enrollment is or was ultimately completed. This paragraph shall have no impact on prior or future collection of such information if collected for EQUIFAX products or services outside of any 2017 BREACH RESPONSE SERVICES AND PRODUCTS.

50. EQUIFAX, including by or through any partner, affiliate, agent, or third party, shall not use any information provided by consumers (or the fact that the consumer provided information) to enroll, or to attempt to enroll, those consumers in the 2017 BREACH RESPONSE SERVICES AND PRODUCTS to sell, upsell, or directly market or advertise its FEE-BASED PRODUCTS OR SERVICES. Nothing in this paragraph, or in this Judgment, shall relieve EQUIFAX of any obligation, or prevent EQUIFAX from complying with its obligations, under federal and/or state law to offer and/or advertise security freezes.

51. Consistent with, and as required by federal law, EQUIFAX shall provide information regarding security freezes on its website. EQUIFAX shall not dissuade consumers from placing or choosing to place a security freeze. Should EQUIFAX offer any standalone product or service as an alternative with substantially similar features as a security freeze (e.g., Lock & Alert), it shall not seek to influence or persuade consumers to choose the alternative product or service instead of a security freeze.

52. EQUIFAX shall not require consumers to agree to arbitrate disputes with EQUIFAX or waive class action rights or any other private right of action against EQUIFAX when receiving or enrolling in any 2017 BREACH RESPONSE SERVICES AND PRODUCTS.

53. **Dedicated Resources for Continued 2017 BREACH RESPONSE:** For a period of three (3) years from the EFFECTIVE DATE, EQUIFAX shall devote reasonable and sufficient resources focused on administering its efforts to support consumers related to the 2017 DATA BREACH ("2017 BREACH RESPONSE"), including but not limited to:

a. Maintaining all consumer-facing internet tools and applications in such a manner that they work reliably and quickly;

b. Establishing and maintaining sufficient staffing levels to handle the volume of consumer traffic;

c. Training employees to provide relevant, useful, and accurate information to consumers who contact EQUIFAX regarding the 2017 DATA BREACH;

d. Promptly handling requests by consumers to place fraud alerts or security freezes consistent with, and as required by, federal law; and

e. Ensuring that the online resources are compliant with the Americans with Disabilities Act (ADA).

54. EQUIFAX shall make the following digital communications available in Spanish, Chinese, Tagalog, Vietnamese, Arabic, French, and Korean: (1) within sixty (60) days of content being finalized, all webpages that EQUIFAX makes available on its website, or on any website that it operates or controls that are dedicated to describing the terms of this Judgment and any benefits available under the Judgment; (2) all legally-required consumer notices regarding any future data breach that are made available on its website, or on any website that it operates or controls; and (3) all notices and claim forms that are made available on any website operated by the settlement administrator. EQUIFAX may satisfy its obligation under this paragraph by providing an automated translation function on the applicable web page(s) which automatically translates all content capable of being translated by the selected translation tool, which, at a minimum, shall translate text appearing directly on the website.

55. **Placing Freezes for PROTECTED INDIVIDUALS:**

a. Pursuant to Paragraph 51 and consistent with, and as required by, federal law, EQUIFAX shall provide information regarding security freezes on its webpage, including information on placing a security freeze on behalf of PROTECTED INDIVIDUALS.

b. EIS shall place, temporarily lift, and remove a security freeze for a PROTECTED INDIVIDUAL consistent with and as required by federal law.

c. EIS shall make good faith efforts to evaluate methods by which representatives of PROTECTED INDIVIDUALS may place, temporarily lift, or remove freezes on behalf of PROTECTED INDIVIDUALS and submit any required documentation via a secure online connection on EQUIFAX's website and take steps to implement such method(s) to the extent they are reasonably feasible and can be accomplished in a manner that complies with federal law.

56. **Consumer Assistance Process:** As part of or in addition to that which is required by federal and state law, EIS shall continue to offer direct assistance, processes, and informational resources to United States consumers who have questions about their EIS CREDIT FILE, who wish to place a fraud alert and/or security freeze on their EIS CREDIT FILE, or who have or may have been the victim of fraud or identity theft. These processes shall include the ability for consumers to contact EIS online, by toll-free phone numbers, and by United States mail, or any other reasonably accessible means established by EIS to communicate directly with consumers.

a. At a minimum, EIS shall:

i. Handle consumer complaints regarding identity theft or fraudulent activity, which may include dedicated teams to review and handle referred complaints by the Consumer Financial Protection Bureau, Federal Trade Commission, or other equivalent federal agency, and the Alabama Attorney General;

ii. Provide direct assistance and informational resources, including, for example, sample template letters and checklists, to help consumers understand their EIS CREDIT FILES and submit disputes related to their EIS CREDIT FILES;

iii. Assist consumers in fulfilling requests for fraud alerts and placing, temporarily lifting, or removing a security freeze on their EIS CREDIT FILE, as well as provide information on how to contact the other CONSUMER REPORTING AGENCIES to place, temporarily lift, or remove a security freeze;

iv. Fulfill its responsibilities to REINVESTIGATE consumers' disputes that information on their EIS CREDIT FILE is inaccurate or incomplete including, as appropriate, escalating disputes for fraud and identity theft to agents specially trained in fraud and identity theft protection;

v. Maintain enhanced consumer dispute results letters to assist consumers in understanding the basis and results of EIS's REINVESTIGATION process, including the actions taken by EIS as a result of the consumer's dispute, the role of the FURNISHER in the REINVESTIGATION process, the results of the dispute including any modified or deleted information, and the options the consumer may take if dissatisfied with the results of the REINVESTIGATION;

vi. Provide informational resources on what supporting and relevant consumer documents may assist a consumer in disputing information on his/her EIS CREDIT FILE and the methods available for consumers to submit documents;

vii. Assist consumers who contact EIS in understanding the basis for when EIS declines to block or rescinds a block of information previously disputed as a result of an alleged identity theft;

viii. Assist consumers disputing inaccurate or fraudulent information and/or accounts by facilitating dispute or REINVESTIGATION requests with FURNISHERS via the Automated Consumer Dispute Verification (ACDV) process; and

ix. Refer consumers to available federal, state, and/or local resources for additional information about consumer rights and identity theft protection measures, such as the sources found at https://www.identitytheft.gov.

b. EIS shall provide direct assistance to members of the United States armed forces, including without limitation members of the National Guard and military reserve, (collectively “Service Members”), or their spouses or other dependents (collectively “Military Families”). At a minimum, EIS shall train a department or group to: help Service Members and Military Families review their EIS CREDIT FILES; review complaints regarding identity theft or fraudulent activity; and help Service Members and Military Families place a security freeze on their EIS CREDIT FILES and implement active duty alerts.

c. EQUIFAX shall designate a department or group to act as the point of contact for the Alabama Attorney General to directly contact and which will provide assistance to consumers who have submitted complaints to the Alabama Attorney General's Office. This department or group shall be trained in the specific provisions of this paragraph.

d. EQUIFAX shall develop a method to identify and track consumer complaints related to the 2017 DATA BREACH and report these metrics to the MULTISTATE LEADERSHIP COMMITTEE as part of the Consumer Remedies Reports required by Paragraph 62 of this Judgment.

e. Disclosure of the Consumer Assistance Process

i. EQUIFAX shall CLEARLY AND CONSPICUOUSLY disclose on its website the following components of the Consumer Assistance Process: the existence of the processes and informational resources offered by EQUIFAX; the content of and how to access an EIS CREDIT FILE; the methods to request a fraud or active duty alert, or take advantage of any security freeze feature on an EIS CREDIT FILE; the methods to dispute the accuracy or completeness of an item on an EIS CREDIT FILE; and informational materials for Service Members and Military Families. EQUIFAX may comply with this paragraph by: (1) maintaining a dedicated website page that describes or provides the resources set forth above; and (2) providing the consumer with a link to said dedicated website page.

ii. For telephone calls with consumers related to the 2017 DATA BREACH, EQUIFAX shall train staff to be prepared to discuss or address in appropriate circumstances: the existence of the processes and informational resources offered by EQUIFAX; the content of and how to access an EIS CREDIT FILE; the methods to request a fraud or active duty alert, or take advantage of any security freeze feature on an EIS CREDIT FILE; the methods to dispute the accuracy or completeness of an item on an EIS CREDIT FILE; and informational materials for Service Members and Military Families. EQUIFAX shall also maintain documentation of this training.

f. EQUIFAX shall maintain reasonable and sufficient staffing levels, resources, and support necessary to respond to foreseeable consumer contact volume.

g. The Alabama Attorney General agrees that it shall not commence any action, the purpose of which would be to establish a violation of this paragraph or a finding of contempt with respect to this paragraph, until on or after December 31, 2019, subject also to the requirements of Paragraph 82.

57. **Declining to Block Information in a CREDIT FILE:** If EIS declines to block, as that term is used in FCRA, or rescinds any block on, the information in a CREDIT FILE that the consumer identifies as information that resulted from an alleged identity theft, EIS shall provide the consumer with additional steps the consumer can take if the REINVESTIGATION of such information results in the information remaining on the consumer's CREDIT FILE, including his/her ability to utilize the Escalated Identity Theft Block Process set forth in Paragraph 58. EIS can choose to satisfy this provision by drafting a form letter to send to consumer that provides this information. This paragraph shall not limit or restrict EIS's ability to designate a dispute filing frivolous or abusive disputes pursuant to 15 U.S.C. § 1681i(a)(3). The Alabama Attorney General's Office agrees that it shall not commence any action, the purpose of which would be to establish a violation of this paragraph or a finding of contempt with respect to this paragraph, until on or after December 31, 2019, subject also to the requirements of Paragraph 82.

58. **Escalated Identity Theft Block Process:** If a consumer complains to a State Attorney General that EIS declined to either block information or rescind the block of information, the Alabama Attorney General may send such complaint to the department or group designated pursuant to Paragraph 56(c) of this Judgment. Upon referral, EIS will review and process the consumer's identity theft report and shall take appropriate action to block the noted information or decline to block or rescind a block, as applicable, from the consumer's EIS CREDIT FILE. This paragraph shall not limit or restrict EIS's ability to designate a dispute filing frivolous or abusive disputes pursuant to 15 U.S.C. § 1681i(a)(3).

59. **Consumer Transparency:** EQUIFAX shall post on the homepage of any website owned or controlled by EQUIFAX: a notice that details categories of the PERSONAL INFORMATION EQUIFAX collects and maintains, including NON-FCRA INFORMATION; how EQUIFAX collects the PERSONAL INFORMATION; how EQUIFAX uses the PERSONAL INFORMATION; how EQUIFAX protects the PERSONAL INFORMATION; whether EQUIFAX shares the PERSONAL INFORMATION with others, and if so, what PERSONAL INFORMATION is shared and the categories of persons or entities with whom the PERSONAL INFORMATION is shared; and whether consumers have control over their PERSONAL INFORMATION, and if so, what kind of control they have and how to exercise the control. If EQUIFAX's PERSONAL INFORMATION practices change, the notice shall be updated to reflect those changes. EQUIFAX may comply with this paragraph by including this information in its online privacy notices.

60. Unless otherwise specified herein, Paragraphs 42 through 59 shall apply for seven (7) years from the EFFECTIVE DATE.

ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY GENERAL

61. **Third-Party Assessment:** During the time period established in Paragraph 13, EQUIFAX shall obtain from an independent third party an initial assessment, followed by biennial assessments of the Information Security Program required under the terms of this Judgment (the "Third-Party Assessments"). The Third-Party Assessments required by this paragraph shall be conducted by a third-party (the "Third-Party Assessor").

a. The findings of each of the Third-Party Assessments shall be documented in individual reports (the "Third-Party Assessor's Reports") that shall:

i. Identify the specific administrative, technical, and physical safeguards maintained by EQUIFAX's Information Security Program;

ii. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering EQUIFAX's size and complexity, the nature and scope of EQUIFAX's activities, and the sensitivity of the PERSONAL INFORMATION maintained on the EQUIFAX NETWORK; and

iii. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by EQUIFAX meet the requirements of the Information Security Program.

b. EQUIFAX may fulfill its assessment and reporting obligations under this paragraph by providing a copy of the Third-Party Assessor's Report required under the FTC Stipulated Order For Permanent Injunction and Monetary Judgment and the CFPB Stipulated Order For Permanent Injunction and Monetary Judgment (the "Federal Security Assessment Report") to the California Attorney General's Office during the time period set forth in Paragraph 13. The California Attorney General's Office may provide a copy of the Federal Security Assessment Report received from EQUIFAX to the Alabama Attorney General's Office upon request.

c. Any Third Party Assessor's Report provided pursuant to this paragraph and all information contained therein, to the extent permitted by the laws of the State of Alabama shall be treated by the Alabama Attorney General's Office as confidential; shall not be shared or disclosed except as described in subsection b; and shall be treated by the Alabama Attorney General's Office as exempt from disclosure under the relevant public records laws of the State of Alabama. In the event that the Alabama Attorney General's Office receives any request from the public to inspect any Third Party Assessor's Report provided pursuant to this paragraph or other confidential documents under this Judgment and believes that such information is subject to disclosure under the relevant public records laws, the Attorney General's Office agrees to provide EQUIFAX with at least ten (10) days

advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that EQUIFAX may take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with the notice requirements contained in Paragraph 81. Nothing contained in this subparagraph shall alter or limit the obligations of the Alabama Attorney General that may be imposed by the relevant public records laws of the State of Alabama, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to the Alabama Attorney General except with respect to the obligation to notify EQUIFAX of any potential disclosure.

62. **Consumer Relief and Internal Metrics Report:** EQUIFAX shall prepare a report regarding its compliance with Paragraphs 53, 55, and 56 ("Consumer Remedies Report") as outlined below.

a. The reporting periods for the Consumer Remedies Reports must cover: (1) the first one-hundred and eighty (180) days after the EFFECTIVE DATE for the initial Consumer Remedies Report; and (2) each one-year period thereafter for the following five (5) years.

b. The Consumer Remedies Reports shall include the following information and metrics:

i. An organizational chart identifying the individuals employed or contracted by EQUIFAX to respond to consumer complaints related to the 2017 DATA BREACH as specified in Paragraph 56(d) and complaints submitted through a State Attorney General as specified in Paragraph 56(c), identified by their titles with a number designating how many staff are assigned to each position;

ii. A description of the training EQUIFAX provides to first-line employees or contractors responsible for directly responding to consumers;

iii. A count of the number of complaints EQUIFAX received, broken down by telephone, email, or regular mail, in which the consumer's complaint relates to the 2017 DATA BREACH as specified in Paragraph 56(d);

iv. The number of fraud alerts placed on EIS CREDIT FILES for United States consumers;

v. The number of security freezes placed, temporarily lifted, or permanently removed on EIS CREDIT FILES;

vi. The number of security freezes placed on behalf of PROTECTED CONSUMERS on EIS CREDIT FILES;

vii. The number of complaints received by EQUIFAX from the Alabama Attorney General's Office pursuant to Paragraph 56(c); and

viii. For the complaints listed in subsection vii EQUIFAX shall indicate whether they were resolved within fifteen (15) business days.

c. Each Consumer Remedies Report must be completed within sixty (60) days after the end of the reporting period to which the Consumer Remedies Report applies. EQUIFAX shall provide a copy of the Consumer Remedies Report to the California Attorney General's Office within ten (10) business days of the completion of the Consumer Remedies Report.

d. The California Attorney General's Office may provide a copy of the Consumer Remedies Reports received from EQUIFAX to the Alabama Attorney General upon request.

e. The Consumer Remedies Reports and all information contained therein, to the extent permitted by the laws of the State of Alabama: shall be treated by the Alabama Attorney General's Office as confidential; shall not be shared or disclosed except as described in subsection (d); and shall be treated by the Alabama Attorney General's Office as exempt from disclosure under the relevant public records laws of the State of Alabama. In the event that the Alabama Attorney General's Office receives any request from the public for a Consumer Remedies Report or other confidential documents under this Judgment and believes that such information is subject to disclosure under the relevant public records laws, the Alabama Attorney General's Office agrees to provide EQUIFAX with at least ten (10) days advance notice before producing the information, to the extent permitted by state law (and with any required lesser advance notice), so that EQUIFAX may

take appropriate action to defend against the disclosure of such information. The notice under this paragraph shall be provided consistent with the notice requirements contained in Paragraph 81. Nothing contained in this subparagraph shall alter or limit the obligations of the Alabama Attorney General that may be imposed by the relevant public records laws of the State of Alabama, or by order of any court, regarding the maintenance or disclosure of documents and information supplied to Alabama Attorney General except with respect to the obligation to notify EQUIFAX of any potential disclosure.

IV. DOCUMENT RETENTION

63. EQUIFAX shall retain and maintain the reports, records, exceptions, information and other documentation required by Paragraphs 31.a), 36.c), 37, 40.a), 40.f), 40.h), 40.i), 61, and 62 for a period of no less than seven (7) years.

V. CONSUMER RESTITUTION

64. **Consumer Restitution Fund:**

a. EQUIFAX shall pay the ATTORNEYS GENERAL an amount of at least Three Hundred Million Dollars ($300,000,000), and no more than Four Hundred and Twenty-Five Million ($425,000,000), for the purpose of providing restitution to AFFECTED CONSUMERS, including the cost of the Three-Bureau Credit Monitoring Services set forth in Paragraph 43 and the monitoring for minors set forth in Paragraph 45(a).

b. The payment/s required by this paragraph may be satisfied in its or their entirety by Equifax Inc. making the payments described in subsection (a) into a fund (the "Consumer Restitution Fund") established pursuant to a court-approved settlement in the MULTI-DISTRICT LITIGATION that pays for restitution and redress to AFFECTED CONSUMERS that includes the Three-Bureau Credit Monitoring Services set forth in Paragraph 43 and the monitoring for minors set forth in Paragraph 45(a) and may also include other restitution and redress to AFFECTED CONSUMERS provided through the MULTI-DISTRICT LITIGATION.

c. The Consumer Restitution Fund shall be established and administered, payments shall be made by Equifax Inc., and consumer restitution shall be disbursed from the Consumer Restitution Fund in accordance with the terms of the court-approved settlement in the MULTI-DISTRICT LITIGATION.

d. If the FTC and the CFPB jointly issue a written notice of termination pursuant Section XI(A) of the FTC Stipulated Order For Permanent Injunction and Monetary Judgment and Section XI.I of the CFPB Stipulated Order For Permanent Injunction and Monetary Judgment, the Alabama Attorney General and EQUIFAX agree that the payment/s required by this paragraph may instead be satisfied in its or their entirety by:

i. EQUIFAX making payments in accordance with the terms of the FTC and CFPB Stipulated Orders For Permanent Injunction and Monetary Judgment. Such amounts shall be deposited into a fund and administered by the FTC or its designee in accordance with the terms of the FTC and CFPB Stipulated Orders for Permanent Injunction and Monetary Judgment to be used for consumer restitution and redress on behalf of the FTC, CFPB, and ATTORNEYS GENERAL; and

ii. The MULTISTATE LEADERSHIP COMMITTEE and EQUIFAX will coordinate with the FTC and/or CFPB so that AFFECTED CONSUMERS receive materially similar restitution as that set forth in Paragraphs 43 and 45(a) of this Judgment.

VI. MONETARY PAYMENT

65. No later than thirty (30) days after the EFFECTIVE DATE, Equifax Inc. shall pay a total of One Hundred and Seventy-Five Million Dollars ($175,000,000.00) to the ATTORNEYS GENERAL, which is to be divided amongst the ATTORNEYS GENERAL. The amount apportioned to Alabama is to be paid by Equifax Inc. directly to the Alabama Attorney General in an amount to be designated by and in the sole discretion of the MULTISTATE LEADERSHIP COMMITTEE. The amounts and wiring instructions shall be provided to Equifax Inc. no later than seven (7) days after the EFFECTIVE DATE. If the Court has not

entered this Judgment by the EFFECTIVE DATE, Equifax Inc. shall make the payment within thirty (30) days of the EFFECTIVE DATE or within fourteen (14) days of the entry of the Judgment, whichever is later. The money received by the Alabama Attorney General pursuant to this paragraph may be used for purposes that may include, but are not limited to, attorneys' fees, and other costs of investigation and litigation, or be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Alabama Attorney General.

VII. RELEASE

66. Following full payment of the amounts due under this Judgment, the Alabama Attorney General shall release and discharge EQUIFAX and its directors, officers, and employees from all civil claims alleged in the Complaint, and any civil claims that it could have brought based on EQUIFAX's conduct related to the 2017 DATA BREACH under the Deceptive Trade Practices Act, Sections 8-19-1 through -15 of the Code of Alabama; the Alabama Data Breach Notification Act sections 8-38-1 through -12 of the Code of Alabama; the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; and any state credit reporting law, or common law claims, including those concerning unfair, deceptive, or fraudulent trade practices. Nothing contained in this paragraph shall be construed to limit the ability of the Alabama Attorney General to enforce the obligations that EQUIFAX has under this Judgment.

67. Notwithstanding any term of this Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 66 as to any entity or person, including EQUIFAX:

a. Any criminal liability that any person or entity, including EQUIFAX, has or may have to the States.

b. Any civil or administrative liability that any person or entity, including EQUIFAX, has or may have to the States under any statute, regulation or rule giving rise to, any and all of the following claims:

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

c. Any private right of action.

68. Nothing in this Judgment shall be construed as excusing or exempting EQUIFAX from complying with any state or federal law, rule, or regulation, nor shall any of the provisions of this Judgment be deemed to authorize or require EQUIFAX to engage in any acts or practices prohibited by any law, rule, or regulation.

VIII. NO ADMISSION OF LIABILITY

69. **Violations of Law:** In stipulating to the entry of this Judgment, EQUIFAX does not admit to any violation of or liability arising from any state, federal, or local law.

70. **Admissions of Fact:** EQUIFAX does not admit to any fact alleged in the Complaint, except admits that on March 8, 2017, it received notification of a vulnerability in Apache Struts open-source software (CVE-2017-5638) prior to the 2017 DATA BREACH.

71. Nothing contained in this Judgment shall be construed as an admission or concession of liability by EQUIFAX, or create any third-party beneficiary rights or give rise to or support any right of action in favor of any consumer or group of consumers, or confer upon any person other than the parties hereto any rights or remedies. By entering into this Judgment, EQUIFAX does not intend to create any legal or voluntary standard of care and expressly denies that any practices, policies, or procedures inconsistent with those set forth in this Judgment violate any applicable legal standard. This Judgment is not intended to be and shall not be construed as, deemed to be, represented as, or relied upon in any manner by any party in any civil, criminal, or administrative proceeding before any court, administrative agency, arbitration, or other tribunal as an admission, concession, or evidence that EQUIFAX has violated any federal, state, or local law, or that EQUIFAX's current or prior practices related to the 2017 DATA BREACH or its information security program is or was not in accordance with any federal, state, or local law.

IX. GENERAL PROVISIONS

72. Nothing herein shall be construed to exonerate any failure to comply with any provision of this Judgment after the EFFECTIVE DATE, or to compromise the authority of the Alabama Attorney General to initiate a proceeding for any failure to comply with this Judgment.

73. Nothing in this Judgment shall be construed to limit the authority or ability of the Alabama Attorney General to protect the interests of Alabama or the people of Alabama. This Judgment shall not bar the Alabama Attorney General or any other governmental entity from enforcing laws, regulations, or rules against EQUIFAX for conduct subsequent to or otherwise not covered by this Judgment. Further, nothing in this Judgment shall be construed to limit the ability of the Alabama Attorney General to enforce the obligations that EQUIFAX has under this Judgment.

74. Nothing in this Judgment shall be construed as relieving EQUIFAX of the obligation to comply with all state and federal laws, regulations, and rules, nor shall any of the provisions of this Judgment be deemed to be permission to engage in any acts or practices prohibited by such laws, regulations, and rules.

75. EQUIFAX shall deliver a copy of this Judgment to, and otherwise fully apprise, its Chief Executive Officer, Chief Technology Officer, Chief Information Security Officer, each of its Business Information Security Officers, Patch Supervisor designated pursuant to this Judgment, General Counsel, and Board of Directors within ninety (90) days of the EFFECTIVE DATE. To the extent EQUIFAX replaces any of the above listed officers, counsel, or Directors, EQUIFAX shall deliver a copy of this Judgment to their replacements within ninety (90) days from the date on which such person assumes his/her position with EQUIFAX.

76. EQUIFAX shall pay all court costs associated with the filing of this Judgment.

77. EQUIFAX shall not participate in any activity or form a separate entity or corporation for the purpose of engaging in acts or practices in whole or in part that are prohibited by this Judgment or for any other purpose that would otherwise circumvent any term of this Judgment. EQUIFAX shall not knowingly cause, permit, or encourage any other persons or entities acting on its behalf, to engage in practices prohibited by this Judgment.

78. EQUIFAX agrees that this Judgment does not entitle it to seek or to obtain attorneys' fees as a prevailing party under any statute, regulation, or rule, and EQUIFAX further waives any right to attorneys' fees that may arise under such statute, regulation, or rule.

79. This Judgment shall not be construed to waive any claims of sovereign immunity Alabama may have in any action or proceeding.

80. If any portion of this Judgment is held invalid or unenforceable, the remaining terms of this Judgment shall not be affected and shall remain in full force and effect.

81. Whenever EQUIFAX shall provide notice to the Alabama Attorney General under this Judgment, that requirement shall be satisfied by sending notice to:

Michael G. Dean
Assistant Attorney General
Office of the Alabama Attorney General
501 Washington Avenue
P.O. Box 300152
Montgomery, Alabama 36130-0152.

Any notices or other documents sent to EQUIFAX pursuant to this Judgment shall be sent to the following addresses:

Chief Legal Officer
Equifax Inc.
1550 Peachtree Street, N.W.
Atlanta, Georgia 30309

Phyllis Sumner
King & Spalding LLP
1180 Peachtree Street, N.E.
Suite 1600

Atlanta, Georgia 30309

Zachary Fardon
King & Spalding LLP
444 West Lake Street
Suite 1650
Chicago, Illinois 60606

All notices or other documents to be provided under this Judgment shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its designee(s) or address(es) by sending written notice to the other party informing them of the change.

82. If the Alabama Attorney General reasonably believes that EQUIFAX has failed to comply with any of Paragraphs 9 through 63 of this Judgment, and if in the Alabama Attorney General's sole discretion the failure to comply does not threaten the health or safety of the citizens of the State of Alabama and/or does not create an emergency requiring immediate action, the Alabama Attorney General shall provide notice to EQUIFAX of such alleged failure to comply and EQUIFAX shall have thirty (30) days from receipt of such notice to provide a good faith written response, including either a statement that EQUIFAX believes it is in full compliance with the relevant provision or a statement explaining how the violation occurred, how it has been addressed or when it will be addressed, and what EQUIFAX will do to make sure the violation does not occur again. The Alabama Attorney General may agree to provide EQUIFAX with more than thirty (30) days to respond. The Alabama Attorney General shall receive and consider the response from EQUIFAX prior to initiating any proceeding for any alleged failure to comply with this Judgment.

83. In the event that technological or industry developments or other intervening changes in law or fact cause EQUIFAX to believe that elimination or modification of this Judgment is warranted or appropriate, EQUIFAX will provide notice to the Alabama Attorney General. If the Parties reach a mutual agreement that elimination or modification of a provision is appropriate, they may jointly petition the Court to eliminate or modify such provision. If the Parties fail to reach an agreement, EQUIFAX may petition the Court to eliminate or modify such provision.

84. Jurisdiction is retained by the Court for the purpose of enabling any party to the Judgment to apply to the Court at any time for such further orders and directions as may be necessary or appropriate for the construction or the carrying out of this Judgment, for the modification of any of the injunctive provisions hereof, for enforcement of compliance herewith, and for the punishment of violations hereof, if any.

85. The Clerk is ordered to enter this Judgment forthwith.

Done and ordered this ___ day of July, 2019.

Circuit Judge

APPROVED:

FOR THE PLAINTIFF:

The State of Alabama
Steve Marshall
Attorney General

By:

/s/ Michael G. Dean

Michael G. Dean
Assistant Attorney General

Office of the Attorney General
Consumer Interest Division
P.O. Box 300152
501 Washington Avenue
Montgomery, Alabama 36130-0152
Telephone: (334) 353-0415
Fax: (334) 242-2433
Email: mdean@ago.state.al.us

Date: July 19, 2019

FOR THE DEFENDANT:

Equifax, Inc.

By:

/s/ John J. Kelley III

John J. Kelley III
Chief Legal Officer
Equifax, Inc.
1550 Peachtree Street, N.W.
Atlanta, Georgia 30309

Date: July 18, 2019

COUNSEL FOR DEFENDANT,
EQUIFAX, INC.:

/s/ J. Andrew Pratt

J. Andrew Pratt
Local Counsel for Equifax, Inc.
Alabama Bar No. ASB-3507-J
King & Spalding LLP
1180 Peachtree Street, N.E.
Suite 1600
Atlanta, Georgia 30309

Date: July 18, 2019

/s/ Phyllis Sumner

Phyllis Sumner
King & Spalding LLP
1180 Peachtree Street, N.E.
Suite 1600
Atlanta, Georgia 30309

Date: July 18, 2019

/s/ Zachary Fardon

Zachary Fardon
King & Spalding LLP
444 West Lake Street
Suite 1650
Chicago, Illinois 60606

Date: July 19, 2019

Schedule of Substantially Identical Agreements

Equifax Inc. entered into substantially identical agreements with the attorneys general of all states, Puerto Rico and the District of Columbia, except for the states of Indiana and Massachusetts. Differences between the agreements include the state attorney general that is the party thereto, the contact information for each state, specific statutory references applicable to each state and the amount of the aggregate payment set forth therein which is to be paid to each state. Collectively, these agreements provide for a total aggregate payment of $180.5 million to these jurisdictions.

Pursuant to Instruction 2 of Item 601(a) of Regulation S-K, a copy of only one of these agreements is filed.